THE ACCESS AND DELIVERY PARTNERSHIP

UNDP

TOOLKIT FOR ENSURING RIGHTS-BASED AND ETHICAL USE OF DIGITAL TECHNOLOGIES

IN HIV AND HEALTH PROGRAMMES

The views expressed in this publication are those of the authors and do not necessarily represent those of the United Nations, including UNDP, or UN Member States.

UNDP is the leading United Nations organization fighting to end the injustice of poverty, inequality, and climate change. Working with our broad network of experts and partners in 170 countries, we help nations to build integrated, lasting solutions for people and planet.

Learn more at undp.org or follow at @UNDP.

Copyright © UNDP 2025. UNDP HIV and Health Group.

THE ACCESS AND
DELIVERY PARTNERSHIP

TOOLKIT FOR ENSURING RIGHTS-BASED AND ETHICAL USE OF DIGITAL TECHNOLOGIES

IN HIV AND HEALTH PROGRAMMES

Contents

Introduction

Digital technologies are transforming health systems, offering unprecedented opportunities to improve health care access, quality and health equity. From telemedicine and AI-driven clinical decision-making to mobile health apps and big data analytics, these innovations hold immense potential to accelerate toward universal health coverage (UHC) and the Sustainable Development Goals (SDGs). However, without appropriate governance, digital and AI health solutions can also exacerbate inequalities, infringe on privacy, undermine human rights and reinforce biases – for example when AI relies on unrepresentative data or operates without transparency.

The United Nations (UN) has consistently advocated for digital transformation to be grounded in human rights and equity. The Secretary-General's Roadmap for Digital Cooperation[1] emphasizes inclusive, safe and rights-based approaches to digital technologies. The UN AI Advisory Body[2] warns against unchecked AI deployment in sensitive health care applications where algorithmic errors or biases could have life-threatening consequences. These frameworks stress that health technologies must be transparent, accountable and designed to bridge rather than widen existing digital divides.

The United Nations Development Programme (UNDP) supports countries in building inclusive, ethical and sustainable digital societies guided by its Strategic Plan[3] and Digital Strategy,[4] reiterating our commitment to support digital transition using a rights-based approach that is centred on human agency and human development. UNDP's HIV and Health Strategy[5] aims to reduce inequalities, strengthen governance and expand access – reducing digital divides and improving health outcomes and health equity. UNDP plays a critical role in working with countries and communities to navigate this digital transition responsibly and develop governance frameworks that align digital and AI health solutions with international human rights and data protection standards. UNDP's work in digital health focuses on ensuring that technology improves equity and serves the most marginalized, aligns with human rights, gender equality, data protection standards, upholds informed consent and safeguards against algorithmic bias and discrimination.

This Toolkit for ensuring rights-based and ethical use of digital technologies in HIV and health programmes complements the UNDP Guidance on the rights-based and ethical use of digital technologies in HIV and health programmes.[6] The Guidance document outlines key ethical, human rights and technical considerations for countries adopting digital technologies for health, detailing human rights risks, norms and standards, and provides a practical checklist for assessment. The Toolkit is practical guidance for UN staff, governments, partners, technology developers, and civil society organizationsfor implementing ethical and rights-based digital health solutions. The Toolkit is organized in six easy-to-access modules. Each module addresses a key issue, outlining definitions, ethical principles, key considerations and recommendations that align with the comprehensive framework in the Guidance document.

---

1 Report of the Secretary-General Roadmap for Digital Cooperation (https://www.un.org/en/content/digital-cooperation-roadmap/).

2 Governing AI For Humanity: Final Report, 2024 (https://www.un.org/en/ai-advisory-body).

3 UNDP Strategic Plan: 2022–2025 (https://strategicplan.undp.org/).

4 UNDP Digital Strategy 2022–25 (https://digitalstrategy.undp.org/).

5 Connecting the Dots: Towards a More Equitable, Healthier and Sustainable Future: UNDP HIV and Health Strategy 2022–2025 (https://www.undp.org/publications/connecting-dots-towards-more-equitable-healthier-and-sustainable-future-undp-hiv-and-health-strategy-2022–2025).

6 Guidance on the rights-based and ethical use of digital technologies in HIV and health programmes (https://www.undp.org/sites/g/files/zskgke326/files/2021–07/UNDP-Guidance-on-the-rights-based-and-ethical-use-of-digital-technologies-in-HIV-and-health-programmes-EN.pdf).

It is important to build trust in digital technology and AI – both for health systems and their beneficiaries. As digital technologies and AI reshape health care, there is a critical question in the balance: will they become tools for equity or instruments of exclusion? The recently published **Human Development Report 2025**[7] also outlines several important implications of AI for health, spanning opportunities, challenges, and policy considerations. While AI in health fosters enhanced diagnostics, early detection, personalized and preventive care, the report also identifies several key challenges in using AI in health care across technical, ethical, social and systemic considerations. By embedding human rights principles and accountability mechanisms into every stage of digital health innovation and AI, these powerful tools can be harnessed for more inclusive health systems and better health outcomes for all.

[7] Human Development Report 2025 (https://hdr.undp.org/content/human-development-report-2025).

Acknowledgement

This Toolkit was developed by the UNDP Digital Health for Development Hub with support from the Access and Delivery Partnership, which is funded by the Government of Japan. It was produced under the overall guidance of Mandeep Dhaliwal, Director of the UNDP HIV and Health Group. The content was compiled and edited by Tim France, Communications Specialist, UNDP.

We would like to extend our special appreciation to Allan Maleche (Legal Expert at Kenya Legal and Ethical Issues Network on HIV and AIDS) and Boyan Konstantinov (UNDP Policy Specialist) for sharing their invaluable insights knowledge and experience.

It also benefitted from inputs and guidance from the following experts:

Manish Pant (UNDP Policy Specialist, Digital Health)

Ketki Bhatia (UNDP Program Analyst, Digital Health)

Ian Mungall (UNDP Program Analyst, HIV and Health)

Heather Doyle (UNDP Regional Team Lead, HIV and Health, Bureau for Asia and Pacific)

Amitrajit Saha (UNDP Regional Team Lead, HIV and Health, Africa)

Marina Smelyanskaya (UNDP Regional Team Lead, HIV and Health, Central Asia)

Karin Santi (UNDP Regional Team Leader, HIV and Health, Latin America)

Elfatih Abdelraheem (UNDP Regional Team Lead, HIV and Health, Arab states)

Kathryn Johnson (UNDP Policy Specialist, HIV and Health Group)

Sean O Connell (UNDP Security and Human Rights Specialist)

Justus Eisfeld (Human Rights and Economic Development expert, Koppa)

Sara (Meg) Davis (Digital Health and Rights expert, Digital Health and Rights Project)

Aditia Taslim (Advocacy officer, International Network of People who Use Drugs)

Alistair Shaw (Global Health and Development Specialist, The Global Fund).

Any views expressed in this document are not necessarily those of these individuals or of any organizations or institutions with which they may be affiliated.

How to use this toolkit

The toolkit is designed to provide practical guidance for a diverse audience, including UNDP staff, governments, partners, technology developers and civil society organizations, who are involved in implementing ethical digital health solutions.

The toolkit serves as a quick reference tool. You can easily navigate the six modules listed in the table of contents. Each module addresses a key issue and outlines definitions, rationales, learning objectives, ethical principles, key considerations, and relevant recommendations. To further enhance practical application, the Checklist from the Guidance document is incorporated as Annex 1, serving as a practical tool for assessing key ethical and rights considerations in adopting digital HIV and health technologies and helping users apply its principles to real-world scenarios. Additionally, the Toolkit incorporates practical case studies, to illustrate and share real-world experiences, further supporting users in applying these principles to concrete situations and strengthening understanding and capacity.

Each module is structured to systematically guide users from understanding the topic and its ethical foundations, to considering practical implementation questions, and finally, outlining actionable recommendations for ethical and rights-based digital health initiatives:

Learning objectives: Outlines the specific knowledge and understanding participants will gain from engaging with the module's content, such as defining key concepts and identifying risks or strategies.

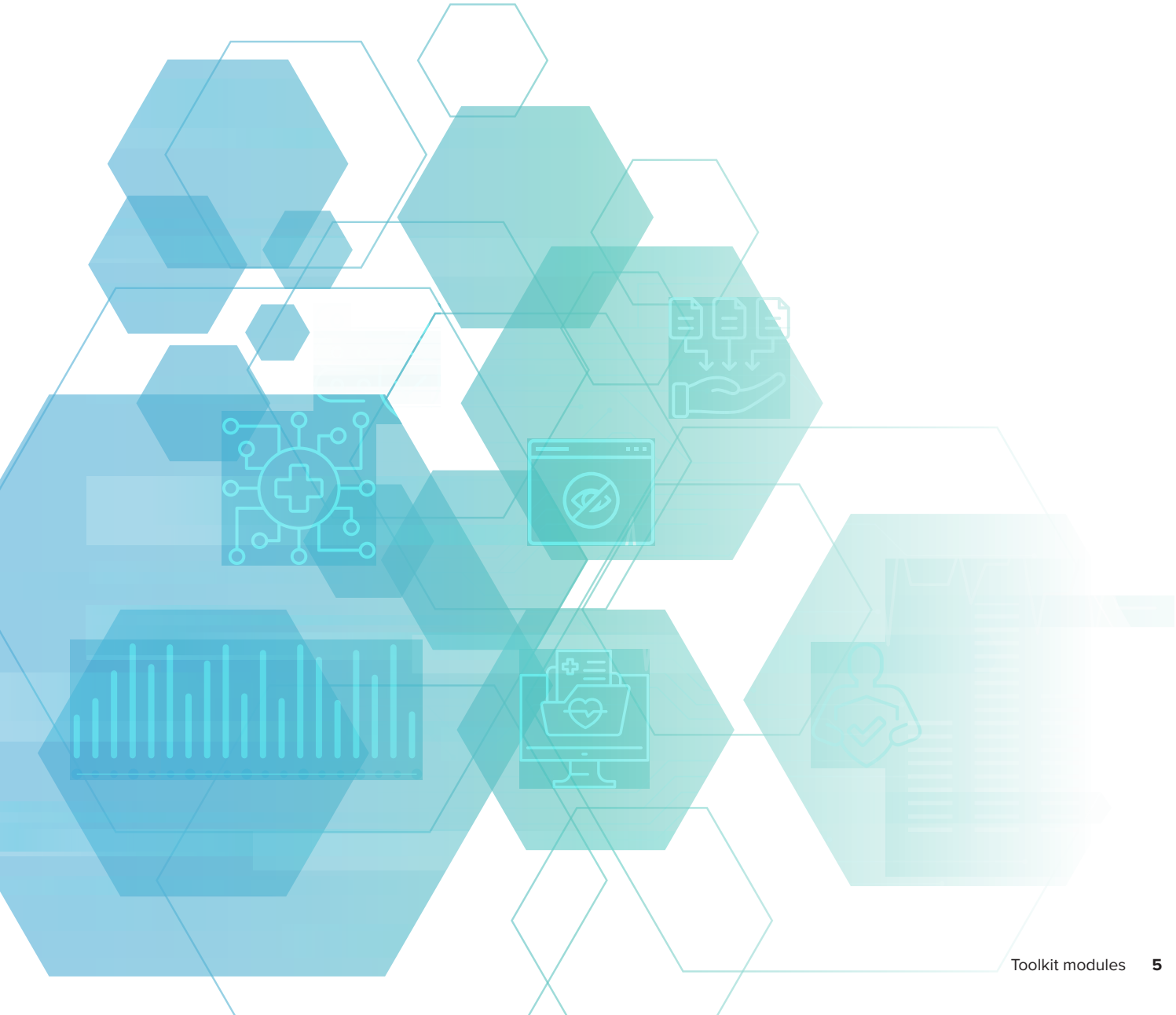
Ethical rationale and principles: Provides the foundational reasoning for the importance of addressing the module's topic, highlighting potential harms like privacy violations or discrimination, and listing the core ethical principles that should guide responses.

Key considerations and adoption: Offers essential practical considerations and guiding questions to ensure the responsible, ethical, and rights-based adoption and implementation of digital health technologies within health programmes.

Relevant recommendations: Details actionable steps and policies for governments, organizations, and other stakeholders to uphold human rights, promote equity, and mitigate risks in the context of digital health technologies.

Additionally, the toolkit can be used as a resource for workshops aimed at orienting participants to its use in their day-to-day work. Annex 2 provides a practical facilitation guide for a 90-minute workshop, specifically designed for UNDP country and regional teams and staff working on health, HIV and/or digital innovation, but adaptable for mixed teams. This workshop format uses guided discussions and interactive activities, such as case studies, to build staff understanding and capacity on ethical digital health issues in an interactive setting. The workshop leverages the main toolkit document and its checklist (Annex 1) for assessing key ethical and rights considerations as reference tools, helping participants become familiar with the content and learn to apply its principles to real-world scenarios.

Toolkit modules



Module 1. Data related issues

This module underscores the critical importance of data privacy, security and the prevention of algorithmic bias in digital health technologies for HIV and health programs. It highlights that without responsible governance, digital tools can exacerbate inequalities, infringe on privacy, and undermine human rights, especially when AI systems lack transparency or rely on unrepresentative data. The core ethical rationale stresses that data breaches violate privacy and erode trust, while bias can lead to systemic mistreatment or exclusion of marginalized groups. The module emphasizes the need for clear informed consent, robust security measures, and transparency in data processing. Its recommendations largely urge governments to establish and enforce privacy laws and regulations that safeguard personal data, prevent misuse, and ensure equity and non-discrimination.

Learning objectives

- Defining data privacy and security in the context of digital health technologies used in HIV and health programmes.
- Identifying key risks and ethical principles related to safeguarding personal health data.
- Defining algorithmic bias and understanding how it can lead to discrimination in digital health.
- Identifying potential sources of bias in datasets and algorithms and discussing strategies for mitigation.

Ethical rationale and principles

Data breaches and biased digital systems both pose serious risks to human rights in health care. Breaches of personal data violate individuals' right to privacy and can erode trust in health systems, while bias in datasets and algorithms may result in the systemic mistreatment or exclusion of marginalized groups. Without responsible governance, digital health tools – particularly those driven by AI – can exacerbate inequalities, infringe on privacy, and reinforce harmful biases, especially when they rely on unrepresentative data or lack transparency.

Autonomy	Freedom of expression	**Non-discrimination**
Bodily autonomy	Harm reduction	**Privacy**
Civic space	Inclusion	Purpose limitation
Data justice	Information rights	Social justice
Dignity	Justice	Sovereignty
Equity	**Non-maleficence**	Transparency

Key considerations and adoption

Ethical

- Are there clear informed consent requirements for data collection? Consent should be freely given, specific, informed, and unambiguous, and the request presented should be in clear and plain language, with the purpose explicitly specified.
- Ensure transparency in data processing so that the data subject can monitor the process and the data controller can create and improve security features. Explicit measures should be in place to ensure transparency in the development and implementation of digital technologies, as well as the use of data collected (including any agreements with private actors).

Social

- Assess the potential for bias or discrimination due to access to and use of digital technologies for health interventions.
- Ensure that the technology is tailored to take into account user experience based on gender, sex, ethnicity, disability, or other major factors (e.g., being a member of a key population group).
- Are there mechanisms in place to monitor and address discriminatory outcomes resulting from the use of digital health technologies?
- Are there safeguards to mitigate risks of discrimination or other rights abuses for marginalized groups?

Technical

- Ensure appropriate security, as well as data integrity and accuracy in data processing methods.
- Implement safeguards to ensure data security, such as anonymization or pseudonymization, as well as the encryption of personal data.
- Conduct security audits related to data storage, transfer, and access as part of technical considerations.
- Are there robust measures in place to ensure the security of personal data, including against unauthorized access, loss, alteration, or misuse?

Relevant recommendations

- Governments should ensure that the use of digital technologies for HIV and health programmes uphold the rights to health and to benefit from scientific progress, specifically advancing equity in terms of availability, accessibility, acceptability and quality, which includes safeguarding data.
- Governments should update and/or enact privacy laws, policies and regulations to safeguard the integrity and security of personal information/data.
- Governments should proactively identify and mitigate risks to non-discrimination in access and availability of technologies, as well as privacy and confidentiality. Where private actors are involved, hold businesses to account in identifying, mitigating and redressing discriminatory outcomes.
- Governments must regulate the collection and storage of personal information – these measures must be effective to prevent unauthorized disclosure or use of personal information.
- Governments must also regulate the control and ownership of data collected through new technologies to prevent misuse and exploitation, as well as ensure informed consent and privacy.

- States should consider legal principles and standards such as the rights of the data subject, criteria for data collection and processing (i.e. lawfulness, fairness, transparency, purpose limitation, data minimization, storage limitation, integrity, accuracy, accountability), data security (i.e. safeguards, anonymization, encryption, transparency), and heightened protections for sensitive data categories.
- Maximize the interoperability of digital health technologies and systems, but enact safeguards to protect personal information from being modified or accessed beyond the specified health purposes, especially for criminalized or highly stigmatized groups.

Case study

Privacy and Security for mHealth Projects in South Africa

→ Challenge

mHealth in South Africa refers to the use of mobile technology to support health care delivery, particularly in areas with limited access to traditional health care services. Some of the major challenges related to privacy and security in the mHealth projects in South Africa include:

- Data privacy and security risks: Sensitive health data transmitted via mobile devices is vulnerable to breaches.
- Legal compliance: Navigating complex legal frameworks like the National Health Act and the Protection of Personal Information (POPI) Act.
- User consent and control: Ensuring informed consent, data accuracy, and user rights to access, correct, or delete their data.
- Technical cafeguards: Implementing adequate security measures to prevent unauthorized access or data loss.
- Cross-border data transfers: Ensuring data sent outside South Africa is protected under equivalent legal standard

→ Solution

Following steps were implemented to address the challenges of privacy and security in the mHealth project:

1. Legal framework alignment which included adherence to the POPI Act and National Health Act provisions. Under the legal framework, the Health Normative Standards Framework (HNSF) for interoperability and security was also defined and implemented.
2. User account portals were created with authentication (e.g. PINs, passwords).
3. Web-based portals to explain the data collection process to users and obtain/manage user consent.
4. Security measures like use of encryption and secure data storage. This also included contracts with third-party processors to ensure compliance with security standards and regular risk assessments and updates to security protocols.
5. Checklist for POPI compliance was created to highlight clear documentation of data use and define data retention policy. Other parameters like guidelines on direct data collection from users, mechanisms for data correction and deletion, and restrictions on direct marketing without consent was also added.

Source: Privacy and Security for mHealth Projects in South Africa (https://www.measureevaluation.org/resources/publications/fs-15-151/at_download/document).

Module 2. Use of digital health technologies

This module addresses crucial challenges in the equitable and safe use of digital health technologies, specifically focusing on 'function creep' – the misuse of data beyond its original purpose – and the 'digital divide' that prevents equitable access. It highlights that data misuse can violate privacy and lead to discrimination or worse health outcomes for marginalized groups, while unequal access can worsen existing health disparities. The module emphasizes the need for technologies that are truly needed, accessible, and inclusive, ensuring clear limitations on data use and robust safeguards against function creep. Recommendations largely focus on governments to bridge the digital divide, enact purpose limitation, and maximize interoperability while protecting personal information.

Learning objectives

- Explaining the concept of the digital divide and its implications for equitable access to digital health technologies.
- Identifying barriers to access faced by marginalized groups and discussing strategies to promote equity.
- Defining function creep and understanding its potential harms, particularly in the context of sensitive health data.
- Explaining the principle of purpose limitation and identifying measures to prevent the repurposing of data.

Ethical rationale and principles

Function creep – the use of data beyond its original purpose – can lead to serious privacy violations and data breaches. When confidential health information becomes accessible to a wider group of potentially biased end-users, it may result in discrimination and worse health outcomes. Data collected for health purposes should be strictly limited to health-related uses and must not be repurposed for surveillance, immigration enforcement, or unrelated profiling.

At the same time, the lack of equitable access to digital health tools risks exacerbating existing health disparities. The global digital divide reflects broader socioeconomic inequalities, where women and other marginalized groups often face structural barriers to accessing and using digital technologies. Without deliberate efforts to ensure inclusion, digital health initiatives may leave these populations further behind.

Insufficient protection of digitized health data compounds these risks. Marginalized groups are particularly vulnerable to criminalization, stigma, discrimination, and even violence when their data is accessed by law enforcement or the courts without adequate safeguards. Robust data protection measures are essential to prevent misuse and protect the rights and safety of those most at risk.

Autonomy	Freedom of expression	Non-discrimination
Bodily autonomy	**Harm reduction**	Privacy
Civic space	**Inclusion**	**Purpose limitation**
Data justice	Information rights	**Social justice**
Dignity	Justice	Sovereignty
Equity	Non-maleficence	Transparency

Key considerations and adoption

Ethical

- Ensure there are clear limitations on how collected data will be used and that these are communicated to users.
- Ensure data collection aligns with a legitimate purpose that is clearly specified and agreed to by the data subject (purpose limitation).
- Data collected should be the minimum amount necessary for the legitimate purpose (data minimization).

Social

- Ensure user accessibility and availability of the digital technologies, considering infrastructure needs like internet access, cell phone coverage, and electricity/power.
- Consider the availability, accessibility, and cost of hardware (e.g. computer, cell phone) and software needed.
- Consider availability and accessibility for marginalized populations, accounting for factors such as socioeconomic status, gender, race, and membership of a key population.
- Ensure that the technology is available to, and appropriate for, vulnerable communities, including those in prisons, closed settings, internally displaced, refugees, or informal settlements.
- Ensure that effective, non-digital options are also available and accessible to all, especially for end-users who may be unable to access or use digital technologies.
- Will the end-user incur any costs for using this technology, and if so, is it affordable and/or covered by insurance?

Technical

- Assess whether the digital health technology is needed to resolve a critical issue or barrier within the HIV response or health system, and if there is evidence of its effectiveness.
- Consider the digital technology as a tool within a broader system to facilitate more effective HIV and health responses, avoiding replication of inefficiencies or exacerbation of inequity if the underlying system has flaws.
- Conduct a health technology assessment to validate technical aspects, clinical considerations, and systems compatibility. This assessment should also assess the risks for bias or discrimination because of access to and use of digital technologies for health interventions.
- Provide incentives for interoperability of systems that encompass strong privacy and data protections.

Relevant recommendations

- Uses of digital technologies for HIV and health programmes must, at a minimum, advance equity in terms of availability, accessibility, acceptability, and quality.
- Governments should proactively identify risks to non-discrimination in access and availability of technologies.

- Governments should ensure that the development and use of digital health technologies uphold the right to health by addressing availability and accessibility to bridge the digital divide.
- When personal information and/or data are collected with full informed consent, there should be safeguards including 'purpose limitation'.
- The standards and systems for interoperability should have strict limitations to protect against 'function creep'.
- Develop the national digital health strategy in a consultative and transparent manner that accounts for the needs of vulnerable and marginalized communities and those living in urban, rural, as well as crisis and conflict settings.
- Develop, implement, and institutionalize digital literacy training for health care professionals, end-users/communities and other relevant stakeholders to facilitate access and uptake of digital technologies.
- Maximize the interoperability of digital health technologies and systems to facilitate more effective and efficient access and provision of HIV and other health services. However, safeguards must be enacted to protect personal information from being modified or accessed beyond the specified health purposes, especially for criminalized or highly stigmatized groups.
- States should provide access to justice where the right to non-discrimination or other rights have been violated.
- There should be an effective, non-digital option that achieves the same goal for those who are unwilling or unable to use digital technologies, or in case of breakdown of the technology.

Case study

Using digital tools to restore HIV care in wartime Ukraine

→ Challenge

The war in Ukraine has severely disrupted the country's health system, making it extremely difficult for thousands of people living with HIV to access life-saving antiretroviral therapy (ART). The displacement of people and the breakdown of health care infrastructure created an urgent need for a way to reconnect individuals with essential health services.

→ Solution

A digital health intervention (DHI) named **#ARTporuch** ("antiretroviral therapy nearby") was rapidly developed and implemented. It included:

- a **website**
- a **chatbot**
- a **centralized database**
- an **information campaign**

These tools helped war-affected individuals locate the nearest functioning health facilities, both within Ukraine and abroad. The campaign generated over 10 million online impressions, with more than 20,000 website visitors and nearly 3,000 chatbot users. The intervention prioritized data security and adapted continuously to emerging needs. It successfully reconnected thousands of people with HIV to essential health care services. Despite wartime constraints limiting quantitative evaluation, the intervention demonstrated the potential of digital health interventions to support health care access in conflict zones and contributed to health system resilience planning.

Source: Digital health intervention reconnects war-affected people living with HIV to healthcare: Ukraine case study (https://doi.org/10.1093/oodh/oqaf001).

Module 3. Privatization

This module delves into the ethical complexities of health information privatization, particularly concerning the extraction of personal health data from low- and middle-income countries (LMICs) for private gain. It highlights the critical concern that such practices often occur without reciprocal benefit to local health systems, raising significant questions about data ownership, access, and benefit-sharing. The module emphasizes the need for transparent agreements, robust regulatory protections, and mechanisms to ensure that the use of health data by private entities ultimately serves the public health interest and benefits the communities from which it was collected. Recommendations are directed at governments to regulate data control, the private sector to uphold human rights due diligence, and donor agencies to thoroughly vet partnerships to safeguard human rights.

Learning objectives

- Defining the privatization of health data and understanding its implications for public health and individual rights.
- Explaining the concept of global data justice and the ethical concerns related to the extraction and use of health data, particularly those from LMICs.
- Identifying potential risks associated with the involvement of private actors in the collection, storage and analysis of health data, including issues of data ownership, access and benefit-sharing.
- Discussing the importance of data sovereignty and ensuring that health data serves the public good and benefits local health systems.
- Analysing the ethical principles of equity and data justice in the context of digital health initiatives involving private sector partners.

Ethical rationale and principles

- Ethical concerns arise when personal data from LMICs is used to enrich private actors without reciprocal benefit to local health systems.
- The growing role of private digital technology and health care companies in providing health care requires they have an increased understanding of their responsibility to respect human rights in their operations. Risks include issues of data ownership, access and benefit-sharing when private actors are involved.

Autonomy	Freedom of expression	Non-discrimination
Bodily autonomy	Harm reduction	Privacy
Civic space	Inclusion	Purpose limitation
Data justice	Information rights	Social justice
Dignity	Justice	**Sovereignty**
Equity	Non-maleficence	Transparency

Key considerations and adoption

Ethical

- Are there explicit measures in place to ensure transparency in the use of data collected, including any agreements with private actors?
- Do the regulations specifically outline legitimate and lawful purposes for data collection, and are these aligned with serving the public health interest rather than solely private gain?
- Are there clear informed consent requirements that explicitly address the potential sharing or use of data by private entities?
- Are there considerations for data ownership and control, particularly in cross-border collaborations involving private companies?

Social

- Are there mechanisms in place to ensure that the use of health data by private actors benefits the communities from which the data was collected?

Technical

- Are there robust legal and regulatory protections for data privacy and security that hold both public and private actors accountable for data breaches and misuse?

Relevant recommendations

- Governments must regulate the control and ownership of data collected through new technologies to prevent misuse and exploitation, particularly by private actors, and ensure informed consent and privacy.
- Where private actors are involved, hold businesses to account in identifying, mitigating, and redressing discriminatory outcomes, as well as privacy and data security violations (human rights due diligence).
- Private sector and technology companies should prevent or mitigate adverse human rights impacts directly linked to their operations, products, or services, in line with the United Nations Guiding Principles on Business and Human Rights.
- Private sector should develop and enact human rights policy commitments and conduct human rights due diligence.
- Donor agencies should ensure that partnerships with the private sector and technology companies are thoroughly vetted so that they proceed in a manner that best protects and advances human rights, including the rights to health and non-discrimination.
- Advocate for transparency in agreements between public health entities and private companies regarding the collection, use, and sharing of health data.
- Promote the development of data governance frameworks that prioritize the public good and ensure equitable benefits from the use of health data, especially for LMICs.
- Consider the ethical implications of using data from LMICs to enrich private actors without reciprocal benefit to local health systems.

Case study 3

Leveraging private health provider data for governance in LMICs

→ Challenge

Low- and middle-income countries (LMICs) have mixed health systems, where private providers – both formal/informal, for-profit and non-profit – deliver a significant share of services. Effective health system governance depends on having timely, accurate and comprehensive data from all providers. However, integrating routine data from private actors into public systems poses various governance challenges:

- **Limited coverage**: Many private providers – especially informal or small-scale – are not registered or do not routinely report data to public systems.
- **Data gaps and poor quality**: Available data from the private sector is often incomplete, inconsistent, or untimely, particularly in service delivery and surveillance reporting.
- **Fragmentation of data types**: While some infrastructure and financing data exist, routine collection of service level, workforce, and pharmaceutical data is rare.
- **Weak governance linkage**: Where data is collected, it is not always used effectively for governance functions like planning, quality oversight, or epidemic surveillance.
- **Barriers to reporting**: Technical, financial and regulatory barriers hinder private sector compliance with national reporting requirements.

→ Solution

A global scoping review of 26 studies from LMICs identified several strategies implemented to improve the collection and use of routine private health provider data for governance:

- **Integration into national systems**: In countries such as Kenya, Nigeria and Tanzania, private providers were included in national health information platforms like DHIS2, enabling routine reporting alongside public facilities.
- **Expanded data categories**: Beyond infrastructure and financing, some governments also gathered data on service delivery, pharmaceutical stocks, workforce numbers, and disease surveillance – broadening the foundation for governance decisions.
- **Public–Private partnerships**: Collaborations with national insurance schemes, regulatory bodies, and private sector associations helped formalize reporting arrangements and incentivize participation.
- **Governance applications**: Where data was available, governments used it for planning equitable service delivery (e.g. facility mapping), evaluating expenditure trends (e.g. in Morocco and Brazil), and tracking essential medicine availability and pricing (e.g. Zambia).
- **Systematic documentation**: A few countries successfully documented and institutionalized these systems, serving as potential models for others aiming to build integrated, mixed-provider health governance mechanisms.

Source: Uses of private health provider data for governance in low-income and middle-income countries: results from a scoping review (https://doi.org/10.1136/bmjopen-2023–083096).

Module 4. Informed consent

This module highlights the paramount importance of informed consent and individual autonomy in the collection, use, and sharing of health data through digital technologies. It underscores that true consent must be freely given, specific, informed, and unambiguous, presented in clear language, as manipulative or covert data collection practices undermine individual agency and trust. The module emphasizes that failure to uphold consent and privacy can lead to severe human rights violations and deter health-seeking behaviors. Key considerations involve ensuring individuals have full control over their personal information and that data collection adheres strictly to specified, legitimate purposes. Recommendations largely urge governments to establish robust legal frameworks for informed consent and advocate for digital literacy to empower individuals in managing their data rights.

Learning objectives

- Explaining the importance of informed consent and autonomy in the use of digital health technologies.
- Recognizing situations where consent may not be real or meaningful and identifying ways to ensure respect for individual autonomy.

Ethical rationale and principles

A lack of meaningful consent options in digital health systems poses a significant human rights concern. Many users are not offered genuine opportunities to opt in or out, and consent mechanisms are often designed in manipulative ways that undermine autonomy. Even when users attempt to opt out of data-sharing in mobile health applications, their choices may not be respected, or opting out may not be technically possible. This limited opportunity to provide informed consent is widely recognized as a key human rights risk.

Safeguarding privacy and confidentiality – closely tied to informed consent – is essential. When these protections are weak or absent, individuals may face serious rights violations, including misuse of their personal information, loss of dignity, and exposure to harm. Furthermore, such breaches can erode trust in health systems, discouraging people from seeking care and leading to delayed or avoided treatment, particularly among vulnerable populations.

Autonomy	Freedom of expression	Non-discrimination
Bodily autonomy	Harm reduction	Privacy
Civic space	Inclusion	Purpose limitation
Data justice	Information rights	Social justice
Dignity	Justice	Sovereignty
Equity	Non-maleficence	**Transparency**

Key considerations and adoption

Ethical

- Ensure that when using digital health technology, all individuals have agency over themselves and their personal information, and that this information can only be collected with their full informed consent.
- Are there policy or legal requirements that digital technologies for HIV and health programmes must align with ethical considerations such as the obligations of autonomy, consent and privacy?.
- Are there clear informed consent requirements for data collection? Consent should be freely given, specific, informed and unambiguous, and the request presented should be in clear and plain language, with the purpose explicitly specified.
- Data must align with a legitimate purpose that is clearly specified and agreed to by the data subject (i.e. purpose limitation).
- Regarding the rights of the data subject, do applicable laws and policies include the right to be informed of the use of their data?

Social

Is information regarding data collection, use, and sharing accessible and understandable to all users, including those with varying levels of literacy?

Relevant recommendations

- Governments should ensure that all digital technologies for HIV and health programmes are aligned with ethical considerations such as the obligations of autonomy, consent and privacy.
- Governments should establish and implement laws, policies and regulations on informed consent for data collection and use of digital technologies for HIV and health.
- States must regulate the control and ownership of data collected through new technologies to prevent misuse and exploitation, as well as ensure informed consent and privacy.
- UNDP advocates for digital health technologies that do not cause any harm to the user and allows for individual's informed consent on the use of their personal data.
- Investing in creating opportunities for digital rights literacy for communities and individuals helps them understand their rights and take ownership of their data, including the right to withdraw their data from use and to data portability.

Case study

Informed consent in UK hospital

→ Challenge

In 2018–2019, a London NHS Trust piloted a digital health intervention using electronic consent (e-consent) for the Human Papilloma Virus (HPV) vaccination programme targeting adolescent girls. Traditional paper-based consent forms were often lost or not returned, leading to lower vaccination uptake. There were also concerns about accessibility and parental engagement.

→ Solution

A multidisciplinary team developed a theory of change (ToC) framework to guide the implementation and evaluation of the e-consent system. The intervention aimed to improve usability, acceptability, and return rates of consent forms. The ToC approach enabled a mixed-methods evaluation, revealing both successes and challenges – such as issues with embedding the intervention and ensuring parental access. The study highlighted the importance of behavioural science in designing digital consent tools and informed future scaling efforts.

Source: Theory-informed evaluation of digital health interventions: case study reflections on the use of a 'Theory of Change' framework (https://www.bsphn.org.uk/publication/theory-informed-evaluation-of-digital-health-interventions-case-study-reflections-on-the-use-of-a-theory-of-change-framework).

Module 5. Surveillance

This module addresses the complex issue of digital surveillance in health technologies, encompassing both intrusive data collection without consent (e.g., reproductive health information) and public health measures like contact tracing. It highlights the significant risk that such surveillance, particularly when impinging on privacy, can lead to harassment, intimidation, violence, and breaches of bodily autonomy, especially for vulnerable groups in restrictive legal contexts. The module stresses that surveillance measures must be lawful, necessary, and proportionate to public health objectives, with clear informed consent, robust data privacy protections, and transparency. Key recommendations urge governments to update privacy laws to explicitly protect sensitive health data, ensure purpose limitation, and promote the right to erasure to safeguard individual bodily autonomy and dignity.

Learning objectives

- Defining intrusive surveillance in the context of digital health technologies.
- Explaining the importance of reproductive privacy and bodily autonomy in the digital age.
- Identifying potential harms and ethical concerns related to the digital collection and use of sensitive reproductive health data, including menstrual tracking and pregnancy-related information.
- Discussing measures and safeguards needed to protect reproductive privacy and prevent intrusive surveillance in digital health programmes.

Ethical rationale and principles

Data collection and surveillance practices that infringe on human rights – particularly the right to privacy – pose serious risks. When intrusive data is collected without consent and shared inappropriately, it can expose individuals to harassment, intimidation, and even violence. This is especially concerning in restrictive legal contexts, such as for people seeking abortion in countries with significant limitations, where surveillance can lead to violations of bodily autonomy and personal safety. In such settings, unchecked surveillance not only undermines individual rights but also reinforces fear and deters people from accessing essential health services.

Autonomy	Freedom of expression	Non-discrimination
Bodily autonomy	Harm reduction	**Privacy**
Civic space	Inclusion	Purpose limitation
Data justice	Information rights	Social justice
Dignity	Justice	Sovereignty
Equity	Non-maleficence	Transparency

Key considerations and adoption

Ethical

- Are the proposed surveillance measures lawful and for legitimate public health objectives?
- Are the measures strictly necessary and proportionate to the health objectives?
- Are there clear informed consent requirements for data collection, particularly for sensitive reproductive health data? Consent should be freely given, specific, informed, and unambiguous, and the request presented should be in clear and plain language, with the purpose explicitly specified.
- Are there explicit measures in place to ensure transparency in the development and implementation of the technology, as well as in the use of data collected, including any agreements with private actors?
- Are there legal and regulatory protections for data privacy and security (i.e. in collection, storage and use), specifically addressing sensitive health information?
- Are there safeguards to mitigate risks of discrimination or other rights abuses for marginalized groups who may be disproportionately affected by intrusive surveillance?
- Are there user notification requirements?
- If the technology is for a specific, time-limited purpose (i.e. COVID-19 or any outbreaks), is its use time-bound?

Social

Does the surveillance technology involve the meaningful and active engagement of key stakeholders such as civil society and communities in its development, implementation and monitoring?

Relevant recommendations

- When personal information and/or data are collected with full informed consent, there should be safeguards including 'purpose limitation', ensuring data is not used beyond its original, consented purpose.
- Governments should update and/or enact privacy laws, policies and regulations to safeguard the integrity and security of personal information/data, with specific attention to sensitive categories such as reproductive health data.
- Ensure that legal and regulatory protections for data privacy and security explicitly address the risks associated with the collection and use of sensitive health data, such as menstrual tracking and pregnancy information.
- Emphasize the importance of bodily autonomy and dignity in the design and implementation of digital health technologies, ensuring individuals have control over their reproductive health data.
- Ensure transparency in data processing, allowing individuals to understand how their reproductive health data is being used and with whom it is being shared.
- Promote the right to erasure ('right to be forgotten'), allowing individuals to request the deletion of their reproductive health data when it is no longer needed for the original purpose.

Case study

Menstrual tracking apps and digital privacy risks

→ Challenge

The 2022 overturning of *Roe v. Wade* by the U.S. Supreme Court triggered restrictive abortion laws in several states, heightening the risks associated with digital reproductive health tools. Millions of users were routinely using menstrual tracking apps to monitor their cycles, fertility, and pregnancy status – often without full awareness of how their data might be accessed or used.

Key concerns included:

- **Sensitive data exposure:** Menstrual apps collect personal reproductive information such as missed periods, ovulation and potential pregnancies – data that could potentially be used to infer or investigate abortion-related activity.
- **Unclear privacy policies:** Many apps lacked transparent privacy terms or did not adequately explain how user data could be shared with third parties, including advertisers or law enforcement.
- **Legal and social risk:** In states where abortion was banned, fears arose that data from these apps could be subpoenaed or misused to target, intimidate, or prosecute individuals.
- **Inequitable impact:** Communities already facing systemic discrimination – particularly low-income users and people of colour – faced disproportionate exposure to these risks, compounded by limited access to legal protection.

→ Solution

To address the ethical, legal and social risks of digital reproductive surveillance, a combination of regulatory, technical and community-led responses was implemented:

1. **Legal and policy safeguards**
   - **Purpose limitation:** Advocacy groups pushed for legislation to restrict how reproductive health data could be used, ensuring it aligned with the user's original intent.
   - **Right to erasure:** Some jurisdictions promoted legal mechanisms enabling users to request the deletion of their reproductive health data from app providers.
   - **Plain-language policies and consent:** App developers revised privacy policies to make them clearer and introduced explicit, opt-in consent processes for sensitive data.
   - **Data minimization and local storage:** Several apps reduced the scope of data collected and introduced on-device storage options, minimizing exposure to breaches or subpoenas.
2. **Technical and community measures**
   - **End-to-end encryption:** Some apps adopted encryption protocols to ensure user data remained inaccessible even to the app provider.
   - **Open-source alternatives:** New, privacy-first menstrual tracking tools were developed using open-source code, enabling greater user control and transparency.
   - **Public education:** Civil society organizations launched campaigns to increase awareness of digital privacy risks and promote safer app choices.

Sources:

Reproductive privacy requires data privacy (https://www.eff.org/deeplinks/2022/05/reproductive-privacy-requires-data-privacy).
Missed period? The significance of period-tracking applications in a post-Roe America (https://doi.org/10.1080/26410397.2023.2238940).

Module 6. Censorship

This module focuses on digital censorship as a significant threat to the right to freedom of expression and access to health information in the digital sphere. It highlights how governments may limit access to crucial health content, restrict advocacy, or silence human rights defenders, emphasizing that such restrictions should not be amplified by digital technologies. The module stresses the importance of legal frameworks and transparent content moderation policies that ensure individuals can freely seek and share accurate health information, particularly for marginalized groups. Recommendations advocate for governments to uphold information rights, for civil societies to hold governments accountable, and for promoting digital literacy and multi-stakeholder dialogue to counter censorship and ensure open access to health knowledge.

Learning objectives

- Defining freedom of expression in the digital context, specifically concerning health-related information.
- Understanding the importance of the right to seek and share health information online without undue government censorship or intimidation.
- Identifying instances and potential harms of digital censorship in the health sector, including restrictions on SRH information and advocacy.
- Discussing the ethical principles related to information rights and civic space in digital health.
- Analyse the role of different stakeholders in upholding freedom of expression and preventing digital censorship in health programmes.

Ethical rationale and principles

The expansion of censorship poses a growing threat to the right to freedom of expression and access to information. In some contexts, restrictive regimes may limit or block access to critical content, such as information on sexual and reproductive health (SRH), or even criminalize advocacy around these issues. Governments must not misuse their authority to restrict content, silence criticism of public policies, shut down the internet, or impose technical controls that suppress dissent. Such actions not only undermine fundamental rights but also hinder public awareness, weaken accountability, and obstruct the work of human rights defenders and journalists.

Autonomy	**Freedom of expression**	Non-discrimination
Bodily autonomy	Harm reduction	Privacy
Civic space	Inclusion	Purpose limitation
Data justice	**Information rights**	Social justice
Dignity	Justice	Sovereignty
Equity	Non-maleficence	Transparency

Key considerations and adoption

Ethical

- Are there policy or legal requirements that ensure individuals can freely seek, receive and impart information and ideas about health, without fear of censorship or retaliation?
- Are there mechanisms in place to ensure transparency regarding content moderation policies and practices on digital health platforms?
- Are there safeguards to protect individuals and organizations advocating for health rights, including SRH, from online harassment or intimidation?
- Are there considerations for balancing freedom of expression with the need to address misinformation and disinformation in the health domain?
- Are there avenues for appeal or redress for individuals whose health-related expression has been unfairly censored or restricted online?

Social

- Are there measures to ensure access to diverse and accurate health information online, particularly for marginalized groups who may face barriers to accessing information through traditional channels?
- Relevant recommendations
- Governments should ensure that the development and use of digital technologies for HIV and health programmes uphold the rights to health and to benefit from scientific progress, which includes the right to access and share health information.
- Civil societies and communities should actively hold governments accountable for their human rights commitments, including protecting freedom of expression in the digital space.
- Advocate for an enabling national legal and policy environment prior to the adoption of digital health technologies, ensuring protection for freedom of expression and access to information.
- Recognize that restrictive regimes may limit access to SRH content or criminalize advocacy, and work to ensure these limitations are not replicated or amplified in the digital sphere.
- Promote digital literacy to empower individuals to critically evaluate online health information and exercise their right to freedom of expression responsibly.
- Foster spaces for dialogue between governments, the private sector, civil society, and communities to address concerns related to digital censorship and promote open access to health information.

Case study

Censorship of women's health content on social media

→ Challenge

Major social media platforms have systematically censored content related to women's sexual and reproductive health (SRH). Investigations by the Center for Intimacy Justice (CIJ) and others found that posts and advertisements on topics such as menstruation, contraception, menopause and sexual wellness are frequently removed or rejected. Automated moderation systems often misclassify legitimate health content as 'adult' or 'sexual', while comparable content about men's health is routinely allowed. This restricts the ability of health advocates and providers to share accurate, sometimes life-saving, information – particularly affecting women, gender-diverse individuals, and marginalized groups. A lack of transparency and meaningful appeal mechanisms compounds the harm.

→ Solution

CIJ has launched legal proceedings under the *EU Digital Services Act* to push platforms to stop unjustified censorship of SRH content. Key demands include improving algorithms to reduce misclassification, and creating fair verification systems for trusted health organizations. At the same time, civil society groups have mobilized campaigns and open letters urging greater transparency and regulatory oversight. These efforts are prompting broader dialogue among governments, tech companies, and affected communities to ensure that content moderation policies uphold the right to access accurate health information.

Source: Menopause, menstrual cups, vulva, endometriosis, abortion, and UTI aren't bad words... So why are these topics censored by Meta, TikTok, Google, and Amazon? (https://www.intimacyjustice.org/report2025).

Annex 1. Glossary of terms

Algorithmic bias in the context of AI and health systems refers to instances where the application of an algorithm compounds existing inequities in socioeconomic status, race, ethnic background, religion, gender, disability or sexual orientation, amplifying them and adversely impacting inequities in health systems. Coding and AI biases within digital health tools stem from historical biases in medical training, diagnostics, clinical care and patient monitoring, which can persist, leading to the exclusion of marginalized groups based on various factors.

Data privacy and security involves safeguarding personal data against unauthorized access, loss, alteration, or misuse.

A **data breach** is any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

Digital censorship involves government censorship and surveillance that threatens the right to freedom of expression and information. This can include limiting access to information (e.g. relating to sexual and reproductive health rights), restricting content, preventing criticism of government policies, shutting down the internet, or silencing the work of human rights defenders or journalists.

The **digital divide**, also referred to as 'digital exclusion', is the gap between individuals who have access to digital technology and information, and those who do not.

Function creep refers to the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy. There is function creep when data collected for a specific purpose is used for another purpose (e.g. if personal history information for HIV testing or treatment are used to check immigration status). Safety and security risk stemming from function creep risk refers to the vulnerability of marginalized groups to criminalization, stigma, discrimination and violence due to insufficient protection for digitized health data, potentially exacerbated by function creep where data is shared for unintended purposes, including with law enforcement or courts without sufficient safeguards.

Informed consent and autonomy involve ensuring individuals can freely decide how their health data is collected, used and shared, based on clear and sufficient information. Autonomy ensures that all individuals have agency over themselves and their personal information, and that this information can only be collected with their full informed consent.

Privatization of health information and services refers to the extraction of personal health data for private benefit, which in high-income countries may limit the use of these data to strengthen low- and middle-income countries' (LMICs) health systems. Ethical concerns arise when personal data from LMICs are used to enrich private actors without reciprocal benefit to local health systems.

Surveillance in the context of digital health technologies can involve collecting intrusive data such as on menstrual information, trends in the purchase of pregnancy tests and in fertility without consent, and sharing these personal data with profit-seeking parties without consent. It can also refer to public health measures such as population surveillance, case identification, and contact tracing facilitated by digital technologies.

Annex 2. Checklist for assessing key ethical and rights considerations in adopting digital HIV and health technologies

Key considerations	Checklist questions	Yes	More work needed	No
Legal and policy environment Foundational and relevant to **all six modules**	Is there a national digital health strategy? If so, does it incorporate ethical, technical and social considerations for adoption of digital health interventions?			
	Are there policy or legal requirements that digital technologies for HIV and health programmes must align with ethical considerations such as the obligations of beneficence, lawfulness, autonomy, consent and privacy, participation and inclusion, transparency, non-discrimination and equity, and accountability?			
	Is there data protection legislation (separate or incorporated in other laws and policies) that includes data protection when using digital health technologies?			
	Are there privacy laws, policies and regulations to safeguard the integrity and security of personal information/data in digital health technologies?			
	Is there a system for biometric and digital identification that respects privacy and human rights?			
	Are there legal or policy mechanisms in place to advance accountability and justice in the use of digital technologies?			
	Are there policy initiatives to improve digital literacy among users and health care providers?			
	Is there a system to identify and address potential human rights risks associated with digital technologies that have been identified and addressed?			
Threshold questions (modules 2, 5 and 6)	Is this technology needed to address or resolve a critical issue or barrier within the HIV response or health system? Will it facilitate or streamline access and/or quality of facilities, goods and/or services (e.g. considerations of complementarity of systems, technology as a tool for good)?			
	Is there objective evidence on the clinical effectiveness of the proposed technological system or intervention for achieving the proposed HIV or health goal?			
	Is this technology reasonably accessible to the population that should benefit from its design and implementation (i.e. do most people have access to the required device, for example, mobile smartphones)?			
	Has this technology been jointly designed with users? Has a meaningful consultation with, and input from, communities been sought?			
Availability (module 2)	Regarding logistics support, are there technological and other fundamental infrastructure in place to support the implementation and uptake of this technology to meet the HIV or health goal (e.g. access to internet and/or mobile phone coverage throughout the country, even in rural areas)?			

Key considerations	Checklist questions	Yes	More work needed	No
Accessibility (modules 1, 2, 4 and 5)	Regarding user access, do end-users have the hardware (e.g. computers, mobile smartphones) and software necessary for accessing and using this technology?			
	Is the government able to provide access to hardware or software for users and/or areas where it is currently not available or accessible?			
	Will end-users incur any costs for using this technology, and if so, is it affordable and/or covered by insurance?			
	Will the end-user have a right to access their health data from the digital technology for health?			
	Is the technology accessible to people with specific requirements such as persons with disabilities, the elderly and children?			
	Is the technology available to, and appropriate for, vulnerable communities, including but not limited to people in prisons and closed settings, people who are internally displaced, and/or those in refugee or informal settlements?			
Acceptability (modules 1, 2, 4 and 6)	Is the technology available in the desired language?			
	Is it tailored to take into account user experience based on gender, sex, ethnicity, disability or other major factors (e.g. being a member of a key population group)?			
	Is the technology culturally appropriate within various communities?			
	Is training or are resources for training available in plain language and accessible formats to support digital literacy for a specific technology among health care professionals and end-users?			
	Has the specific digital technology been tested, piloted or implemented to achieve the expected HIV or health goal?			
Data privacy and security (all modules)	Regarding data collection: • Are there clear informed consent requirements for data collection? Consent should be freely given, specific, informed and unambiguous, and the request presented should be in clear and plain language, with the purpose explicitly specified? • Do the regulations specifically outline legitimate and lawful purposes for data collection? • Are there data minimization requirements (i.e. collecting the minimum necessary for the legitimate purpose)?			
	Regarding storage and authorized use: • Are there requirements for the data collected to be kept accurate, and if necessary, up to date? • Are there standards that data processing methods ensure appropriate security and data integrity, including anonymization, where relevant, and rigorous processes to ensure authentication for authorized users and encryption? • Are there mandates that personal, identifiable data can only be stored as long as necessary for the specified purpose (e.g. limited retention)?			

Key considerations	Checklist questions	Yes	More work needed	No
	Are there heightened protections for the collection and storage of special categories of data, including genetic data, personal data related to criminal offences, unique identifying biometric data, as well as personal data that reveal a person's racial or ethnic origins, political opinion, religious and other beliefs, health and sexual life?			
	Regarding the rights of the data subject: • Do the applicable laws and policies include the following rights for individuals whose data are collected? • the right to be informed of the use of their collected data; • the right to access stored data; • the right to rectification; • the right to erasure (i.e. the 'right to be forgotten'); • the right to restriction of processing; • the right to be notified of rectification or erasure, or restriction of processing; • the right to data portability; • the right to object; and • rights related to automated decision-making and profiling.			
Health-related surveillance, including contact tracing (modules 1, 3, 4 and 5)	Are the proposed surveillance measures lawful and are they aimed at legitimate public health objectives?			
	Are the measures strictly necessary and proportionate to the health objectives?			
	Are there explicit measures in place to ensure transparency in the development and implementation of the technology, as well as in the use of data collected, including any agreements with private actors?			
	Does the surveillance technology involve the meaningful and active engagement of key stakeholders such as civil society and communities in its development, implementation and monitoring?			
	Are there user notification requirements?			
	Are there legal and regulatory protections for data privacy and security (in collection, storage and use), including the above-mentioned data and privacy requirements?			
	Are there safeguards to mitigate risks of discrimination or other rights abuses for marginalized groups?			
	Is there access to redress and justice for users who may have their rights violated through the use of the technology?			
	Is there an institution or entity that can provide public oversight, review and accountability on the use of the technology?			
	If the technology is for a specific, time-limited purpose (i.e. COVID-19 or any outbreaks), is its use time-bound?			
Non-discrimination (modules 1, 2, 3 and 6)	Can pre-existing laws related to non-discrimination be applied to the impact and uptake of digital technologies?			
	How well are private companies regulated in terms of legal compliance regarding human rights issues? Are there mandatory provisions for human rights due diligence?			

Key considerations	Checklist questions	Yes	More work needed	No
Accountability and access to justice (all modules)	Are private actors required to have policy commitments to human rights and to conduct human rights due diligence in order to be legally compliant with the business regulations within the country?			
	Do individual and entities have the rights to bring cases related to potential discrimination as a result of digital technologies before courts (i.e. are technology-related discrimination claims justiciable?)			
	Are there other mechanisms and or interventions available to support access to justice for technology-related human rights violations (e.g. impartial courts specializing in surveillance issues, training for judges and law enforcement on the use of digital technologies)?			
Important human rights-based approach considerations (all modules)	Have rights holders participated in the design, implementation, governance, monitoring and evaluation of digital health technologies?			
	Does the digital technology for health link to internationally recognized human rights standards and principles?			
	Are there accountability mechanisms such as remedies for rights violations related to the digital health technologies?			
	Does the digital health technology ensure the non-discrimination of people, i.e. is the technology inclusive of all within society, including the most marginalized and those most left behind?			
	Does the digital technology for health lead to the empowerment of rights holders?			
	Regarding the transparency of actions, is the digital technology for health developed, adopted, and implemented in an open and accessible manner that allows for public feedback, consultation and monitoring?			

Annex 3. Facilitation guide for a 90-minute ethical digital health workshop

Purpose and audience

This annex provides a practical **facilitation guide** for UNDP country and regional teams to conduct a **90-minute internal workshop** on the rights-based and ethical use of digital technologies in HIV and health programmes. By using this guide, UNDP country teams can confidently organize and run a 90-minute workshop that is practical, engaging, and impactful. The format is intentionally simple – a facilitated discussion and a case exercise – so that no specialized training expertise is required.

The session is designed to build staff understanding and capacity on ethical digital health issues in an interactive, informal setting. It can be used for in-person workshops or adapted for online sessions (including when the facilitator is remote). **UNDP staff** working on health, HIV, or digital innovation are the target audience, but the format is flexible for mixed teams. The workshop uses a **guided discussion** format with one interactive activity, and it leverages the main toolkit document and its checklist as reference tools throughout the session. This ensures participants become familiar with the toolkit's content and learn to apply its principles to real-world scenarios.

Workshop format and preparation

Format: The workshop is a semi-structured discussion with minimal presentation. Instead of lectures, the facilitator will guide participants through questions and scenarios, prompting them to reflect on key issues. One **interactive activity** (e.g. a case study exercise) is included to apply concepts in practice. The atmosphere should remain informal and participatory, encouraging everyone to share thoughts. This format works for both **in-person** meetings and **online** sessions. If the facilitator cannot be physically present, they can lead via video call – just ensure on-site organizers have the room setup and technology ready.

Preparation: Follow these steps to get ready for the session:

- **Read the Toolkit:** The facilitator (and co-facilitator, if any) should review the main UNDP guidance toolkit on ethical digital health and the annexed **checklist** beforehand. Familiarize yourself with the key ethical principles (e.g. do no harm, privacy, inclusion) and the checklist questions that assess digital health projects. This will build confidence to lead discussions and answer questions.
- **Select a case or project:** Choose a short written **case study** or example to use for the interactive activity. Ideally, pick a scenario relevant to your context – for instance, a plan to roll out a health app or digital patient registry in your country. You can use a real UNDP-supported project (with identifying details anonymized if needed) or a hypothetical scenario. Alternatively, invite participants to bring their **own project ideas** to discuss (e.g. an upcoming digital health intervention they are planning). Ensure the case is concise enough to explain in a few minutes, but rich enough to illustrate ethical questions (e.g. privacy, data use, inclusion of key populations, etc.).
- **Materials:** Prepare any materials needed. For in-person, print a few copies of the **ethical checklist** from the toolkit (or have it displayed on a flipchart/slide) so small groups can refer to it during the activity. For online, have the checklist and key toolkit excerpts ready to screen-share or send as a PDF to participants. If using slides, you might only need 1–3 slides (i.e. title, outline,

possibly the case description or discussion questions). Gather any stationery for in-person (e.g. flipchart paper, markers, sticky notes) or set up virtual whiteboard tools for online (e.g. a shared Google Doc or Miro) if you plan to capture input.

- **Participants:** Invite the relevant team members. Emphasize that no prior expertise is required – **anyone interested in digital health or concerned about its impact** is welcome. If the group is larger than ~10 people, consider breaking into smaller groups for the case study activity to ensure everyone has a chance to speak. For online, set up breakout rooms in advance if needed.
- **Technology (if online or hybrid):** Test the video meeting link, screen-sharing, and any interactive tools beforehand. If participants are in a conference room and the facilitator is remote, ensure there is a good speakerphone or video setup so the facilitator can hear and interact with everyone. Designate a local staff member to assist with on-site logistics or to moderate the chat for questions.

By preparing in advance and keeping the setup simple, country teams can run this session **without external expertise** – the materials in the toolkit will guide the content. The goal is to create a safe, open environment for staff to learn from each other and from the toolkit.

Session outline (90 Minutes)

1. Below is a step-by-step agenda for the 90-minute session. Times can be adjusted, but ensure the total is about an hour and a half. The facilitator should keep track of time so that the discussion stays focused and the group can complete the activity.

2. **Introduction and objectives (10 min):** Welcome everyone and briefly introduce the purpose of the workshop. Explain that the session will explore how we can adopt digital technologies in health programmes while respecting human rights and ethics. Mention that this is an informal, **learning-focused discussion** – *not* a training lecture. If participants don't all know each other, do a quick round of introductions (name, role, and if relevant, experience with digital health). Outline the agenda: a short group discussion of key concepts, a case study activity, and a wrap-up. **Set ground rules** for an open discussion (e.g. respect differing opinions, no question is 'silly', and keep specific project details confidential if needed). Emphasize that the UNDP **guidance toolkit** and checklist will be our reference points during the session, and everyone should feel free to draw from their own experiences or concerns.

3. **Guided discussion – key concepts (15 min):** Start by posing a few broad questions to the group to tap into their understanding and spark interest. For example, ask *"What opportunities do digital tools bring to our HIV and health work?"* and *"What concerns or risks have you heard about?"* Encourage participants to share thoughts. As they respond, highlight the **rights-based principles** from the toolkit in simple terms. Ensure that concepts like **privacy and data protection**, **consent**, **inclusion of marginalized groups**, **equity in access (digital divide)**, **non-discrimination**, and **accountability** are mentioned either by participants or by the facilitator. For instance, if nobody brings it up, the facilitator can say: *"One important principle in the guidance is ensuring informed consent and privacy protections for any health data collected. Why might that be especially important for HIV-related data?"* – letting participants reflect (e.g. stigma or legal risks may arise if data is misused). Jot down key points on a flipchart or shared screen as they emerge. Keep this discussion interactive – rather than lecturing on definitions, use participants' answers to underscore why an ethical, rights-based approach matters (for example, a participant might mention *"not everyone has internet or smartphones"*, opening a conversation on inclusion and accessibility). By the end of this segment, the group should have a common understanding that digital health innovations hold **great promise** but also **perils** if human rights are not safeguarded. Reinforce that the UNDP toolkit was developed to help navigate these issues.

4. **Interactive case study activity (40 min):** Now transition to the main activity where participants will apply the toolkit's **checklist** and ideas to a concrete example. Introduce the chosen **case study or project scenario** (2–3 minutes description). For example: *"Imagine our country office is assisting the Ministry of Health to launch a mobile app that helps people living with HIV schedule clinic appointments and receive medication reminders. Let's explore how to ensure*

this intervention is ethical and rights-based." If using a participant's own project, invite them to give a brief overview. Distribute the printed checklist or share it on screen. **Break the group into smaller teams** (3–5 people each, or pairs if the group is small) to discuss the case. Each team should identify potential ethical and human rights issues in the scenario and suggest how to address them. Encourage them to use the checklist questions as a guide. For instance, teams can go through questions like *"Is this technology truly needed and effective for the problem?"*, *"Will it be accessible to the most vulnerable users?"*, *"Are there safeguards for data privacy and consent?"*, and *"Have end-users been consulted in the design?"*. They don't have to cover every checklist item in detail – suggest focusing on a few key areas due to time. **If online:** you can use breakout rooms; if in-person with a small group, teams can huddle in different corners or simply discuss at the table. Give about **20 minutes** for team discussion. The facilitator should circulate among groups or jump between breakout rooms to answer questions and keep them on track. After 20 minutes, reconvene everyone. Have each team briefly **report back** (2–3 minutes each) on the issues they identified and any suggestions. As each team speaks, the facilitator can draw connections and fill any gaps: for example, if a group didn't mention data security, the facilitator might ask, *"Did you consider what happens if the app's data is breached? How could that affect users?"* – prompting additional input. Use this debrief to reinforce how the checklist helped uncover important considerations. **Note:** If time is tight or the group is smaller, you can do this activity in plenary instead – reading the case and then discussing questions as one group, possibly writing responses on a shared board.

5. **Wrap-up and next steps (15 min):** Conclude the workshop by summarizing the key takeaways. Recap a few points from the case exercise – e.g. *"We saw that even a well-intentioned digital health project can have blind spots, like leaving out those without smartphones or risking privacy breaches, but by asking the right questions (using our checklist) we can plan to mitigate these issues."* Emphasize how **using the toolkit and checklist** is a practical way to integrate a human rights-based approach in daily work. Encourage participants to apply this thinking to their own projects going forward. Ask if anyone has final questions or comments. It's also effective to do a quick **reflection round**: for instance, ask each person to name one insight from today or one action they will take (e.g. *"I will make sure to involve the community in designing our new health info system"*). Finally, point participants to the resources for further reading – the **main toolkit document** and its annexes (like the checklist they used, and this facilitation guide itself) and the more comprehensive UNDP *Guidance on the rights-based and ethical use of digital technologies in HIV and health programmes*. If appropriate, mention that the session can be expanded or repeated with other teams, and that they are encouraged to keep discussing these topics. Thank everyone for their active participation and contributions.

(If time remains, you can optionally show a short video or example from another country illustrating ethical digital health in practice, but this is optional and only if you have extra time.)

United Nations Development Programme
One United Nations Plaza, New York,
NY 10017, USA

UNDP is the leading United Nations organization fighting to end the injustice of poverty, inequality, and climate change. Working with our broad network of experts and partners in 170 countries, we help nations to build integrated, lasting solutions for people and planet.

Learn more at undp.org or follow at @UNDP