CONSOLIDATED GUIDELINES ON PERSON-CENTRED HIV STRATEGIC INFORMATION: STRENGTHENING ROUTINE DATA FOR IMPACT

POLICY BRIEF ON DIGITAL HEALTH DATA

BACKGROUND

In many countries health information systems are in transition from paper-based to digital record-keeping. Digital systems offer opportunities to greatly improve patient-centred care. At the same time, the transition poses new challenges. In the domain of HIV, new guidelines from the World Health Organization (WHO) suggest how to address these challenges and move toward an effective and efficient digital system for client monitoring.

Broadly, the new Consolidated guidelines on person-centred HIV strategic information: strengthening routine data for impact [1] aim to help countries improve how routine patient data are collected, analysed and used. They propose a minimum dataset that captures key events in an individual's interaction with the health system, put forward priority indicators for monitoring a person's health, and make key recommendations for data systems and data use. In addition to the development and use of digital health data systems, the guidelines address HIV prevention, testing and treatment, HIV-related infections, using routine surveillance data to measure programme impact and supplementing routine patient data with data from other sources.

This policy brief summarizes the WHO guidance on digital health data in HIV services. The guidance covers several areas that are acutely important for transitioning from paper-based to digital systems while improving patient outcomes: interoperability, unique identifiers (UIDs) and privacy, security and data access and control.

> Few opportunities for change within the health care system are so wide-ranging as the transition from paper-based to digital systems.

The dramatic growth in, and use of, health data necessitates systematic investment in digital systems. This investment can yield huge benefits: Digital systems simplify the collection and analysis of data and improve the accuracy, reliability, completeness and timeliness of data – improvements can lead to more focused and appropriate care and better continuity of care across providers, facilities, and over time. When strongly underpinned by human rights, values such as the principles for digital development, and considerations of equity, the transition to digital systems has huge potential to improve global health.

Photo: © WHO / Booming - Carlos Cesar

[1] Consolidated guidelines on person-centred HIV strategic information: strengthening routine data for impact. Geneva: World Health Organization; 2022.

Principles for digital development

Design with the user	Be data-driven
Understand the existing ecosystem	Use open standards, open data, open source and open innovation
Design for scale	Reuse and improve
Build for sustainability	Address privacy and security
	Be collaborative

Source: Principles for digital development 2018 (https://digitalprinciples.org/principles/, accessed 23 June 2022).

INTEROPERABILITY

For data to be used effectively, they need to be exchanged among, and understood by, the many different stakeholders in the health care system. Interoperability enables this. It allows data to be shared within a health system, so that health care can be organized around people rather than as separate services. Interoperability is often thought of as *technical* interoperability which covers standards for writing and structuring data, terminologies used in health care, and technical standards for secure data exchange. However, some of the most important initiatives for enabling data use and exchange concern governance. *Organizational* interoperability facilitates efficient management to promote data sharing, alignment of organizational goals and standards through national strategy documents, and ensures that a minimum dataset is shared with the health ministry to inform public health planning. Finally, *legal* interoperability concerns the removal of legal barriers to allow data use and exchange across jurisdictions and to encourage efficient data exchange as individuals move among locations.

A fully interoperable data system improves the responsiveness of health care systems, streamlines reporting for multiple diseases, eases the burden of aggregate reporting of health data, enables real-time use of data, and integrates data among various facilities and agencies, such as community-delivered services.

Key recommendations on interoperability

UPDATE 1. Explicitly build in interoperability standards, data use rules and obligations and transparent data governance in digital health systems to allow the secure exchange and use of health data:

UPDATE a) Use technical, organizational and legal interoperability standards to facilitate data governance and to smooth data exchange and use between health care sector partners.

NEW b) Publish agreed-upon standards, rules, frameworks and conditions for data use by health ministries, partners and civil society to improve transparency, data sharing and use.

UNIQUE IDENTIFIERS

UIDs are numeric or alphanumeric codes used to identify patients in individual-level health data systems. UIDs ensure that each individual can be correctly and repeatedly identified when accessing health care across services and locations. This increases the health care system's responsiveness and efficiency, ultimately improving patient outcomes.

A well-designed UID is free of any personally identifiable information. While UIDs can contribute to efficiency and quality of care, they may risk identifying individuals if the identifier is not free of personal information or if it is linked to such information. This is of specific concern where consensual same-sex sexual activity, sex work or drug use are criminalized and associated with stigma, discrimination and violence. If people are aware – or they suspect – that information on their behaviours or membership in a key population will be recorded, they may hesitate to use services.

Therefore, UIDs must be introduced with strong technical data security standards and secured with robust data security policies and national legal protections. A fully evolved national system of UIDs requires legal, regulatory and policy frameworks to protect data as well as strong enforcement capability and procedures to rapidly address breaches of data security.

The UID provides the anonymous identifier that can be shared across devices, facilities and disease programmes to link data on the same individual.

UIDs should be implemented in a step-wise fashion, reflecting each country's context (Fig. 1), and following a situation analysis to understand the feasibility of different approaches.[2] The initial step is replacing name-based paper records with records labelled with a unique alphanumeric code for each individual without any personally identifying information. Then, digitization of records will require investment in data security to safeguard the expanded use of UIDs.

After data security is ensured, investment is needed to promote data use to improve programmes, such as with analytics and dashboards. Transition to an advanced stage requires commitments to programme sustainability, such as financing and capacity building, and expanding UIDs to link individuals' records across services and facilities, and over time. Currently, the level of adoption of digital data systems in health care varies across countries and may be at different stages of maturation in different districts or disease programmes within countries.

Key recommendations on UIDs

UPDATE 2. Use unique identifiers that replace names and personal information with anonymous alphanumeric codes to allow person-centred data to support a person accessing services over time and across facilities, districts, health and disease programmes:

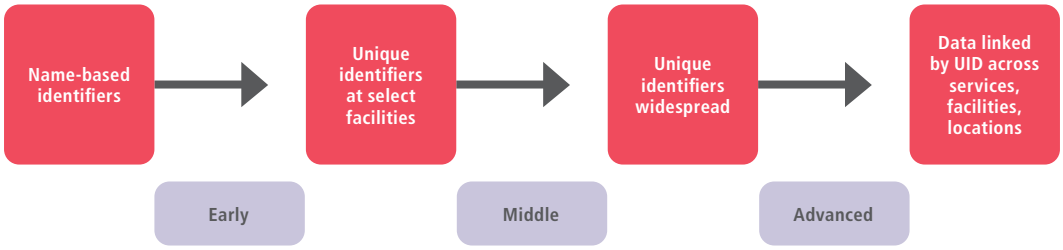
UPDATE a) Unique identifiers, supported by data protection policies, should preserve individual anonymity, thereby separating personal and confidential data from health data that are being routinely shared.

UPDATE b) Unique identifiers should be progressively introduced across facilities, districts, disease programmes and other health care to promote person-centred services.

NEW c) Adopt national technical and legal protections for an individual's unique identifier and for individuals to access the data associated with their unique identifiers.

[2] WHO's Digital adaptation kit (DAK) for HIV provides guidance and a package of tools on moving from paper-based to digital systems to ensure the adherence of WHO guidelines during this transition.

Fig. 1 Broad stages and transitions on the maturation pathway for UIDs



PRIVACY, SECURITY, DATA ACCESS AND CONTROL

The increasing volume, use, and exchange of digital data, along with the concentration of data in centralized data warehouses, heightens both the risks and the consequences of data breaches. Digital health care systems need to be designed from the start, and implemented with, privacy, security and confidentiality in mind. This is especially important for key populations. Who has access to and control over personal health data has serious implications for clients' safety and health outcomes, and building trust with clients is acutely important in marginalized populations. Empowering clients to be partners in improving their own health outcomes is a key benefit of transparent legislation assuring rights-based access and control of one's own health data.

Privacy refers here to the legal protection accorded to an individual to control both access to and use of personal information.[3] Legislation is an important mechanism for ensuring that clients have access to and control of their own health data. Individuals must have rights to access their data and the ability to correct any incomplete or inaccurate data. Legislation should stipulate that only data that are clinically relevant or necessary for clinical management can be collected.

The success of digital systems heavily depends on appropriate strategies for governance and policy that protects data and individual rights.

Privacy provides the overall framework for implementation of both confidentiality and security. Confidentiality is the individual's right to protection of their information during storage, transfer and use to prevent its unauthorized disclosure to third parties. Security refers to the technical approaches to physical, electronic and procedural aspects of the protection of information collected as part of health care services. Security addresses protection of data from both intentional and unintentional disclosure as well as non-availability of data due to system failure or user errors.

Photo: © WHO / Lindsay Mackenzie

[3] The privacy, confidentiality and security assessment tool — user manual. Geneva: Joint United Nations Programme on HIV/AIDS (UNAIDS); 2019 (https://www.unaids.org/en/resources/documents/2019/confidentiality_security_tool_user_manual, accessed 27 October 2022).

Key recommendations on data privacy and security

UPDATE 3. Invest in secure and confidential data systems, protected by policies and rights, with different data security levels for different data elements and different health care users:

UPDATE a) Establish different data security levels for data elements and appropriate data access based on health care needs and data users (care givers, implementers, health ministries, partners and civil society).

NEW b) Personal data should be kept confidential and not be disclosed to unauthorized parties; personal data should be accessible only to the data subject and to other explicitly authorized parties.

NEW c) Security includes suitable policies and regulation, not simply technical security.

NEW d) Patients should have access to their own health data through a portable, persistent, protected personal health record. Over time, person-centred data should support people to increasingly use and shape how their data are used.

NEW e) Both the benefits and risk of data are elevated for key populations. Confidentiality and security issues are, therefore, paramount, and personally identifying data should never be used beyond the care giver and point of access to services if not protected by clear policies and rights.

With the expansion of digital health systems globally, opportunities for the use of person-centred data captured in routine national health information systems will continue to grow. The key areas outlined in this guidance can help to ensure that health data is accessible as clients move locations, is more accurate and comprehensive, can be used in real-time, and that data use and exchange occurs in a secure environment, respecting client privacy and confidentiality. Ultimately, investment in such areas can thereby translate into improvements in patient outcomes and global health.

Photo: © WHO / Blink Media - Nana Kofi Acquah

FOR MORE INFORMATION, CONTACT:

World Health Organization
Department of Global HIV Hepatitis and Sexually Transmitted Infections Programmes
20, avenue Appia
1211 Geneva 27
Switzerland
E-mail: hiv-aids@who.int
www.who.int/hiv

Consolidated guidelines on person-centred HIV strategic information: strengthening routine data for impact. Policy brief on digital health data
ISBN 978-92-4-006435-5 (electronic version)
ISBN 978-92-4-006436-2 (print version)

9789240064355