USAID
FROM THE AMERICAN PEOPLE

Digital Threats to Democracy in the Global Health Sector



Digital threats to democracy are a growing topic of conversation among those in the Democracy, Human Rights and Governance (DRG) sector. However, digital threats to democracy affect all USAID sectors, including economic growth, agriculture, education, and global health. As noted in USAID's Digital Strategy, the increased use of digital tools and technology has brought many opportunities for improved outcomes in USAID partner countries. However, technology also provides an avenue for undemocratic actors to manipulate information, exploit private data, surveil public space, and impinge upon human rights. Building on the findings of the Bureau for Africa's 2021 Democratizing Digital Landscape Assessment, USAID has identified an important need and opportunity to further integrate awareness of digital threats to democracy into its programming. A 2022 digital development portfolio mapping of USAID digital development efforts showed that safeguards to protect privacy, human rights, and democratic freedoms are underrepresented and underreported in USAID-funded projects. This underscores the importance of countering and mitigating digital threats to democracy across USAID programming in sub-Saharan Africa. This document looks into the intersection of digital threats to democracy and the global health sector for a USAID audience with an Africa focus. It offers recommendations for strategically raising awareness of digital threats to democracy and incorporating these considerations into programming, and explores key trends in digital threats to democracy across the global health sector.

How USAID Can Mitigate Digital Threats to Democracy in its Global Health Programming

The benefits of digital health tools[1] in low- and middle-income countries are clear. According to USAID's Vision for Action in Digital Health, they "can improve health outcomes, increase the quality and accessibility of care, address the needs of clients and health workers, reach vulnerable populations, address gender disparities, and improve health equity."[2] McKinsey & Company estimates that African health systems can experience up to a 15 percent increase in efficiency by expanding their use of digital health tools, freeing up billions of dollars to strengthen national health systems.[3] However, as the USAID Vision for Health Systems Strengthening 2030 acknowledges, "Digital transformation comes with risks of increasing inequality, repression, and instability." Identifying and mitigating the potential for digital threats to democracy across USAID's global health portfolio supports high-performing and resilient health systems[4] while promoting open, inclusive, and secure digital ecosystems in USAID partner countries.

1 According to USAID's Vision for Action in Digital Health, digital health is "the systematic application of information and communications technologies, computer science, and data to support informed decision-making by individuals, the health workforce, and health institutions, to strengthen resilience to disease and improve health and wellness for all."

2 A Vision for Action in Digital Health | United States Agency for International Development

3 How digital tools could boost efficiency in African health systems | McKinsey & Company

4 USAID Vision for Health System Strengthening - 2030 | United States Agency for International Development

USAID can play an important role in fighting and mitigating digital threats to democracy through its global health portfolio. The box below highlights key questions to consider during program design. This is followed by specific recommendations for USAID staff based in Washington and USAID Mission staff and implementing partners aiming to address these issues in their global health programming.

Ensuring the use of rights-respecting technologies in USAID global health programming

Digital tools can accelerate development outcomes in USAID partner countries, but they can also pose digital threats to democracy. These threats may not be immediately clear. In considering the range of potential digital threats to democracy in the short- and long-term stemming from digital interventions in global health programming (digital tools, technologies, policies, processes, systems, or other digital ecosystem-oriented interventions), ask the following questions considering three scenarios:

1. impact under the current government,
2. impact if the current government begins or accelerates the process of democratic backsliding, and
3. impact under a new, more authoritarian government.

Questions for consideration:

- How can this intervention promote or be affected by **digital surveillance**?
- How can this intervention promote or be affected by **misinformation, disinformation, or malinformation**?
- How can this intervention promote or be affected by **online censorship**?
- How can this intervention promote or be affected by **internet shutdowns**?
- How can this intervention promote or be affected by **targeted online persecution**?
- How can this intervention promote or be affected by **offline persecution for online behavior**?
- How can this intervention potentially expose individuals to t**argeted harassment or legal issues** based on their gender, identity, or perceived affiliation with a group such as LGBTQI+?
- How can this intervention be positively or negatively affected by **data localization**?
- What are **other potential misuses of this intervention**?

Recommendations for USAID/Washington staff

These recommendations address how USAID/Washington staff can raise awareness of digital threats to democracy within their sectors and USAID portfolios - in this case, global health.

Internal facing

Develop guidance for USAID staff and implementing partners on how to apply the *Donor Principles for Human Rights in the Digital Age* to programming in the global health sector. This will help ensure that USAID does not fund non-rights-respecting technologies.

Fund targeted research to identify how digital threats to democracy manifest in the global health sector such as digital health tools that expose private health data or online censorship of public health information and disseminate it widely across the Agency, including through relevant USAID working groups.

Develop simple and practical tools to aid in identifying, measuring the severity of, and countering digital threats to democracy within the global health sector and disseminate them across USAID Missions.

Incorporate an analysis of digital threats to democracy in all future USAID or USG-wide global health-related strategies or policy documents. These documents can guide policy discussions around countering digital threats to democracy in the global health sector.

Design and provide practical, hands-on training to USAID staff and implementing partners on:

- The risk of digital threats to democracy in the global health sector, with a focus on concrete strategies to identify and mitigate potential digital rights abuses in their programming.
- Assessing cybersecurity risks in their programming and integrating adequate cybersecurity protections into their work, which can prevent or mitigate the effects of digital threats to democracy.[5]

Design and test evaluation methods to measure the impact of digital threats to democracy and associated mitigation strategies in the global health sector, with the objective of developing indicators to incorporate into activity and intervention design.

Gather evidence from USAID-funded programs on how to mitigate the impact of digital rights abuses on the global health sector, in order to replicate or adapt these methods in new programming.

External facing

Build awareness of potential digital threats to democracy in the global health sector among donors, implementers, and other key stakeholders by funding high profile events, publications, and public communications campaigns at the national and international level. This could include working through national digital health governance groups and the Digital Health & Interoperability Working Group.

Coordinate across donors to channel funds into the development or scale up of rights-respecting digital public goods (DPGs) in the global health sector. On the USAID side, this could include using Development Innovation Ventures (DIV) grants to fund the development or scale-up of rights-respecting DPGs for global health.

Develop minimum safety and cybersecurity measures for digital public goods in the global health sector by coordinating across donors, national governments, and other relevant stakeholders.

Recommendations for USAID Mission staff and implementing partners at the country level

These recommendations address how USAID Mission staff can raise awareness of and counter digital threats to democracy in their global health portfolios at the country level.

What does USAID's A Vision for Action in Digital Health 2020-2024 Say About How To Mitigate Digital Threats to Democracy?

"Robust policy and regulatory environments, strong health institutions, and health workforces skilled in the use of digital systems and data relevant to their domain areas, are essential to protecting against and mitigating the unintended or malign uses of digital technologies in the health context."

5 Available USAID resources include: Democratizing Digital Video and Facilitator's Guide; Digital Literacy Sectoral Briefers; Cybersecurity Sectoral Briefers; Digital Government Sectoral Briefers; Principles for Digital Development Training: Health (USAID internal).

Key considerations for USAID when designing or funding digital health interventions:

Track rapid shifts in the local digital ecosystem that may indicate emerging digital threats to democracy, with a particular focus on digital policies impacting the healthcare sector such as data protection or data privacy for health management information systems.

As stated in USAID's A Vision for Action in Digital Health, "USAID also must guard against the abuse or manipulation of digital technology." This means avoiding assistance which may help to create or support systems that could allow governments or other entities such as private sector actors or faith-based health providers to use citizens' genetic or health data against them. USAID can build in safeguards such as policies and processes concerning data anonymization, information access management, and encryption to ensure that USAID investments cannot be used to promulgate digital threats to democracy or risk individual privacies and protections.

"Assess cybersecurity risks and address vulnerabilities in digital health systems to mitigate potential harms," as advised in USAID's Digital Health Vision Technical Guidance Note on Advancing National Digital Health Strategies.

Ensure that all digital health tools that receive USAID funding "align with applicable country privacy and security policies and regulations as well as global best practices to protect against inappropriate access to and misuse of information," according to USAID's Digital Health Vision Technical Guidance Note on Advancing National Digital Health Strategies.

"Prioritize privacy and security needs in all related investments to secure digital systems, protect individuals' personally identifiable and sensitive information, and use data responsibly in alignment with best practices and relevant standards," per USAID's Digital Health Vision Technical Guidance Note on Strengthening Country Digital Health Capacity.

Do not use digital health tools that pose digital threats to democracy in global health programming, including internet-connected medical devices or machines, in alignment with USAID's Cybersecurity/Global Health sector brief.[6]

Provide Digital and Cyber Hygiene Training for all Implementing Partners. The use of simple, routine measures can protect users and their data.

With national governments in USAID partner countries:

- Provide technical assistance (TA) in drafting and implementing national level data protection policies and regulations that extend to the health sector. This aligns with USAID's Vision for Health System Strengthening 2030, which states "At the country level, efforts to secure data must be incorporated not only at the individual and provider levels but also at the national level with general data protection regulations."
- Build capacity among Ministry of Health employees in: 1) designing, procuring, and implementing rights-respecting digital tools for health, and 2) building cybersecurity protections into their health management information systems and other digital health tools.
- Support the Ministry of Health in building a strategic communications department that can: 1) identify health-related disinformation spreading locally and develop targeted, localized campaigns to counter such falsehoods and rumors; and 2) share factual information about topics that are censored online, such as women's reproductive health.
- Work with USAID partner countries to include language in their national digital health strategies on the importance of countering digital threats to democracy in their healthcare sectors.

6 USAID Cybersecurity/Global Health Sectoral Brief

With the creators, designers, or owners of digital health tools:

- Minimize the amount of personally identifiable information (PII) that digital health tools collect on patients.
- Prioritize cybersecurity by design and deploy best-in-class cybersecurity protections when developing new digital health tools, including for electronic medical records.
- Provide TA to ensure that safeguards on digital health tools include physical (i.e. equipment), administrative (i.e. policies, practices, and processes), and technical (i.e. technology) considerations to provide full scale protection.
- Provide TA to ensure that digital health tools "align with applicable country privacy and security policies and regulations as well as global best practices to protect against inappropriate access to and misuse of information," in alignment with USAID's Digital Health Vision Technical Guidance Note on Advancing National Digital Health Strategies.
- "Use data responsibly in alignment with best practices and relevant standards," as instructed in USAID's Digital Health Vision Technical Guidance Note on Strengthening Country Digital Health Capacity.
- Provide TA to ensure that digital health tools do not have the technical capacity to facilitate online surveillance or online censorship.
- Encourage partners to discuss data and privacy concerns in order to find solutions.

With healthcare facilities:

- Deploy cybersecurity best practices to safeguard their digital health tools—including Health Management Information Systems and Electronic Medical Records—to protect patient privacy.
- Provide TA to ensure that safeguards on digital information include physical (i.e. access to the facility itself, access to staff workstations), administrative (i.e. policies, practices, and processes that ensure staff protect personal data), and technical (i.e. technology securities such as passwords) considerations.
- Work with healthcare facilities to ensure that staff are appropriately trained in digital data protection. Facilities should have the knowledge and capacity to provide staff with regular cyber hygiene training and to ensure that best practices are integrated into day-to-day work.
- Use only digital health tools with no known cybersecurity vulnerabilities, which collect only minimum required PII, and that do not promulgate digital threats to democracy.
- Develop and implement strategies to counter highly localized health-related mis- and disinformation, tailored to the populations that they serve.

With healthcare workers:

- Leverage frontline healthcare workers (HCWs) to combat mis- and disinformation efforts by building their capacity to critically assess information sources and to identify mis- and disinformation campaigns within their communities. Consider integrating cyber hygiene modules into HCW training.
- Train HCWs to deploy cyber hygiene best practices in their day-to-day work with patients, such as enabling multi-factor authentication to log into health management information systems.

With civil society:

- Strengthen the capacity of organizations in USAID partner countries to identify and mitigate digital threats to democracy in the global health sector, such as TA and training in leveraging social media listening tools to identify health-related disinformation in specific geographic areas and in identifying cases of online surveillance enabled by digital health tools.
- Monitor healthcare-related mis- and disinformation campaigns on social media in order to design effective programming to counter rumors and falsehoods.

Key Trends in Digital Threats to Democracy Across the Global Health Sector

What does USAID's A Vision for Action in Digital Health 2020-2024 Say About Digital Threats to Democracy?

"USAID recognizes that cyber security, data privacy, and trust are critical to the effective functioning of health institutions. USAID is ready to mitigate the potential harms of digital technology, from enhancing the security of personal identity information as digital health systems become increasingly linked and interoperable with other systems, to countering the influence of actors who seek to use digital-technology assets and infrastructure for malign purposes, managing misinformation and disinformation during the response to pandemics, and promoting our implementing partners' use of secure and reliable digital technologies… USAID will not fund or support national digital health strategies or architectures that enable "digital authoritarianism," in which a repressive government controls the Internet and uses censorship, surveillance, and data/media laws or regulations to restrict or repress freedom of expression, association, religion, and peaceful assembly at scale."

Digital threats to democracy such as data privacy violations, online surveillance, mis- and disinformation, and online censorship can affect health system resilience by compromising patient confidentiality, undermining access to factual health information, and giving cover to governments to punish activists. Current trends around the globe and in sub-Saharan Africa include:

- **Digital tools in the health sector can expose private health data and personally identifiable information (PII)**. As noted in USAID's Vision for Health System Strengthening 2030, "A whole-of-society approach to health system development must also consider the client privacy concerns that may arise from digital transformation efforts." While robust data protection and privacy policies, strong cybersecurity protections, and effective oversight mechanisms are required to safeguard sensitive health data and patient PII, they are not universal across the healthcare sector. Recent Mozilla research shows that 59 percent of mental health mobile applications studied did not protect user privacy, and that privacy protections had worsened over the previous year for 40 percent of these apps.[7] Hacks and breaches of healthcare systems are rapidly increasing, with the United States experiencing a nearly 250 percent increase in large breaches reported to the Department of Health and Human Services over the past four years.[8] Sub-Saharan Africa is not immune. A 2020 cyberattack on South Africa's Life Healthcare disrupted its admissions, email, and business process services.[9] The disclosure of PII and sensitive health data can reduce trust in healthcare systems around the globe, particularly for healthcare seekers in marginalized groups (like the LGBTQI+

7 Shady Mental Health Apps Inch Toward Privacy and Security Improvements, But Many Still Siphon Personal Data | Mozilla

8 HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation | US Department of Health and Human Services

9 South Africa's Life Healthcare hit by cyber attack | Reuters

community) or for those with stigmatized medical conditions. As noted in USAID's Vision for Health System Strengthening 2030, "client privacy must be protected."

- **Some digital health tools can track the movements or behavior of individual users, facilitating online surveillance at scale**. This cuts across all aspects of the global health field. The COVID-19 pandemic brought this issue to the fore around disease surveillance. The original COVID-19 contact tracing apps introduced by Bahrain, Kuwait, and Norway sent the GPS locations of app users to government databases in real time, which would theoretically have allowed these governments to track the movements of its citizens.[10] In all cases, the live location data could be linked to real people because app registration required either a national ID number or a valid phone number.[11] High potential for online surveillance also extends to the reproductive health field. Period tracking apps store information about the menstrual cycles of their users, which in theory can be turned over to local law enforcement or otherwise tapped into by governments, abusive partners, or other malign actors. These examples demonstrate how digital health tools can facilitate online surveillance across the global health sector, as well as their potentially destructive effects on individual patients.
- **Mis- and disinformation spreads falsehoods that can promote disease spread and disincentivize people from seeking care**. Viral mis- and disinformation campaigns during the COVID-19 pandemic, or the "infodemic," illustrate the scope of the problem. In terms of the impact on patient care and health outcomes, the US Surgeon General has reported that misinformation has "led people to decline COVID-19 vaccines, reject public health measures such as masking and physical distancing, and use unproven treatments."[12] In sub-Saharan Africa, Princeton University researchers identified more than 400 instances of false information about COVID-19 circulating on social media from January-September 2020.[13] Some narratives such as one suggesting that police or military forces in Kenya and South Africa were attacking citizens who violated lockdown or curfew sought to instill fear of government institutions, while others sowed mistrust in public health institutions, like the World Health Organization.[14] Other research from Francophone and Anglophone countries in West Africa from late 2020 and early 2021 showed organized efforts to spread disinformation narratives with the involvement of pro-Russian actors.[15] This underscores the importance of identifying and effectively combating health-related social manipulation and disinformation campaigns.
- **Social media platforms censor public health information, particularly on women's health issues and family planning and reproductive health (FP/RH)**. According to 2022 Center for Intimacy Justice research, Meta (Facebook) rejected ads from all 60 businesses it surveyed, which serve women's health and health for people of diverse genders. Half of these companies—which focus on menopause, menstrual health, sexual wellness, pelvic pain, and other related topics— subsequently had their Facebook ad accounts suspended. Accounts offering similar health products for men could seemingly post on Facebook with no issue.[16] Similarly, the "Love Matters" online communities share factual information about FP/RH with young people on social media in eight countries, including the Democratic Republic of the Congo, Kenya, and Nigeria. From 2015-2022, nearly one-third of Love Matters ads on Facebook were rejected for apparently advertising adult products and services, adult content, and disruptive, low quality content.17 The Love Matters Kenya Facebook page was blocked for more than six months in

10 Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy | Amnesty International

11 Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy | Amnesty International

12 Confronting Health Misinformation: The U.S. Surgeon General's Advisory on Building a Healthy Information Environment | Surgeon General of the United States

13 Corona-free? How disinformation could be clouding the true pandemic picture in Africa | Bulletin of the Atomic Scientists

14 Corona-free? How disinformation could be clouding the true pandemic picture in Africa | Bulletin of the Atomic Scientists

15 Disinformation exports: How foreign anti-vaccine narratives reached West African communities online | First Draft

16 Meta's Censorship of Health Ads for Women and People of Diverse Genders | Center for Intimacy Justice

17 The Naked Truth: Meta's Censorship of Sexual Health Information and Advocating to Big Tech for Change | RNW Media

2019-2020, while the Love Matters page for the DRC was disabled in 2022.18 If social media censorship prevents young people from having access to women's health and FP/RH-related information, products, and services, it may affect health outcomes around the globe.

- **National governments can censor or target critics for their online behavior in the name of global health**. At least eight healthcare workers were arrested in Egypt in 2020 after posting online about their concerns with the Government of Egypt's response to COVID-19.19 An activist in Niger was arrested and sentenced to three months in prison for sharing her opinions about the Government of Niger's response to COVID-19 in private WhatsApp messages.20 The Government of Tanzania deployed its existing laws making the dissemination of "false news" illegal to prevent online and print news outlets from reporting on COVID-19 early in the pandemic.21 It banned Mwananchi Newspaper Online for six months in April 2020 after it shared a photo of President Magufuli seemingly violating Tanzania's social distancing rules and banned Kwanza Online TV for 11 months in July 2020 for sharing factual information about COVID-19.22 These examples show how governments can manipulate public health emergencies to promote online censorship and digitally-enabled targeted persecution.

These trends highlight the growing need for USAID and implementing partners to consciously integrate safeguarding into global health programming involving digital tools and technology. To learn about recommendations and trends in digital threats to democracy for other USAID sectors, please refer to the following (to be linked):

- Digital Threats to Democracy - Economic Growth
- Digital Threats to Democracy - Education
- Digital Threats to Democracy - Agriculture

Please contact USAID/AFR/CPG afrdigital@usaid.gov for more information.

18 The Naked Truth: Meta's Censorship of Sexual Health Information and Advocating to Big Tech for Change | RNW Media

19 Egypt: Health care workers forced to make impossible choice between 'death or jail' | Amnesty International

20 Niger: La loi sur la cybercriminalité est un instrument de répression des voix dissidentes | Amnesty International

21 Silenced and Misinformed: Freedom of Expression in Danger During COVID-19 | Amnesty International

22 Silenced and Misinformed: Freedom of Expression in Danger During COVID-19 | Amnesty International