Photo: Raz Jahnpour for USAID/Digital Development Communications

USAID DIGITAL STRATEGY

USAID'S FIRST-EVER DIGITAL STRATEGY CHARTS AN AGENCY-WIDE VISION for development and humanitarian assistance in the world's rapidly evolving digital landscape.

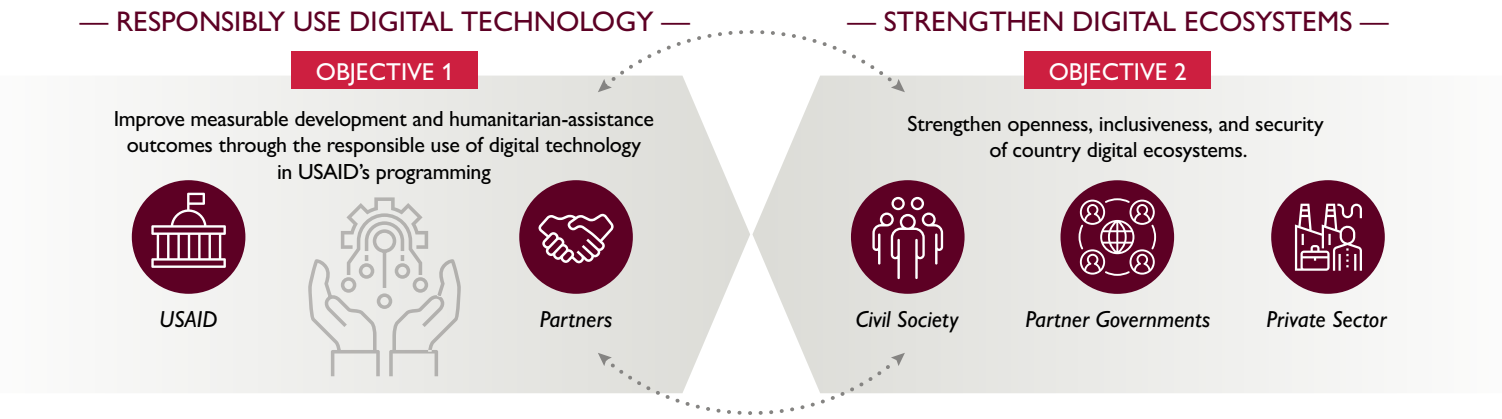
THE DIGITAL REVOLUTION has given way to the promise of a digital world that spurs economic growth, improves health outcomes, and lifts millions out of poverty using new technologies and services. While digital tools present immense potential to advance freedom and transparency, generate shared prosperity, strengthen inclusion, and inspire innovation, it also presents significant risks to privacy and security through competing models of Internet freedom.

STRATEGY GOAL

To achieve and sustain open, secure, and inclusive digital ecosystems that contribute to broad-based, measurable development and humanitarian-assistance outcomes and increase self-reliance in emerging market countries.

The *Digital Strategy* includes two core, mutually reinforcing objectives:

DIGITAL ECOSYSTEM: *stakeholders, systems, and enabling environments that together empower people and communities to use digital technology to gain access to services, engage with each other, or pursue economic opportunities.*



To achieve the overall goal of the *Strategy*, these objectives will be executed through four tracks:

TRACK 1: ADOPT AN ECOSYSTEM APPROACH ▸ **Develop tools and resources** necessary to deliver development and humanitarian assistance effectively in a digital age

TRACK 2: HELP PARTNERS NAVIGATE RISK AND REWARDS ▸ **Build capacity of our partners** to navigate the unique opportunities and risks that digital technology presents across USAID's Program Cycle

TRACK 3: SHIFT TO "DIGITAL BY DEFAULT ▸ **Support implementing partners** in adoption of digital operations

TRACK 4: BUILD THE USAID OF TOMORROW ▸ **Invest in our human capital** to guide the Agency through the digital age

USAID
FROM THE AMERICAN PEOPLE

TRACK 2: HELP PARTNERS NAVIGATE RISK AND REWARDS: CONSIDERATIONS FOR COVID-19 RESPONSE

CLOSING THE GENDER DIGITAL DIVIDE

USAID's first-ever Digital Strategy outlines a path to strengthen open, inclusive, and secure digital ecosystems in all partner countries, and calls on the Agency to "augment our commitment to close the gender digital divide and address the disproportionate harm women and girls face online."

CLOSING THE GENDER DIGITAL DIVIDE IN THE CONTEXT OF COVID-19 AND DEVELOPMENT

The gap between women and men's access to and use of the Internet and mobile phones is significant. As COVID-19 increases countries' reliance on digital services, men will benefit disproportionately to women since they will have greater access to life-saving information. Women and girls not having access to resilience-building information will be left behind, exacerbating existing gender inequalities. While there is pressure to act quickly, gender must be considered across all response and recovery efforts. The decisions made now will have long-term effects on the stabilization and resilience of communities, especially women and girls.

WHAT IS THE CLOSING THE GENDER DIGITAL DIVIDE INITIATIVE?

The Digital Strategy commits USAID to helping build inclusive digital economies, and specifically calls out the need to ensure that women and girls are fully included in the digital ecosystem. Women are, on average, 14 percent less likely to own mobile phones than their male counterparts, and 43 percent less likely to engage online.[1] Empowering women economically and socially is a core tenet of development policy, but persistent—and growing— gaps in women's access to, and use of, digital technology significantly hamper their ability to improve their lives, the stability of their families, and the resilience of their communities. No country will be self-reliant if citizens cannot benefit equally from the gains of a global digital ecosystem.

KEY CONSIDERATIONS FOR THE GENDER DIGITAL DIVIDE IN COVID-19 RESPONSE PROGRAMMING

Questions to ask when designing a digital intervention for COVID-19 response:

- **Will your digital intervention reach vulnerable populations and is it responding to their needs?** Do women and girls have access and full ability to use the digital solution? Will social norms prevent them from using this digital solution – if so, how will programming address and overcome barriers? It is critical to understand the size and shape of the gender digital divide in your specific context (e.g., is it more about access, ownership, employment in ICT fields, financial tools, etc.), noting that it can vary within a country.
- **How can you better use digital tools to ensure that inequalities are not exacerbated in this crisis?** How do you ensure women and girls can access life-saving digital tools and services while mitigating potential harms, like online gender-based violence?
- **How can you ensure all gender identities are being included across the data lifecycle: collection, analysis, sharing?** Are you collecting sex-disaggregated data AND data on intersectionality and social factors, such as age and sexual orientation?

1. AfterAccess, 2018.

Questions to ask partners (continued):

- **How can you work directly with community leaders to create compelling cases for women's technology use – under what conditions would women be allowed to use the Internet?** How can this allowance be expanded over time? Are there technologies or policies that can uniquely support these "use cases"?
- **Could the private sector provide expertise in gender dynamics around technology use and COVID-19 response?** Do they have relevant data on women's access and use of digital technology to better inform COVID-19 response programming?

Similarly, there are risks and opportunities that can arise during a response to a global pandemic and need to be considered. Examples of risks and opportunities related to the Closing the Gender Digital Divide Initiative can include:

RISKS

Exacerbating the gender digital divide. Because the pandemic is increasing society's dependence upon information technology to curb COVID-19 and to keep economies running, the pandemic will substantially increase the cost of digital exclusion for the one billion women currently not using the internet and their families. If men have wider access than women to digital solutions that preserve livelihoods and health, a failure to address the gender digital divide will increase gender inequality.

Increased online and physical harm. Digital technology can provide information, outreach, and support, but only when women and girls can safely access and use the technology. Failure to carefully consider the ramifications of promoting increased digital technology and Internet use is not responsible. Digital intervention should be assessed with a gender lens focused on mitigating potential harm. Digital technology has been linked to violence against women and online sexual harassment. With increased time at home and time spent online, women, and in particular young girls, are at increased risk of online gender-based violence (GBV) and technology-facilitated GBV during the COVID-19 health crisis.

Excluding women and girls from data collection, analysis, and sharing. We need to adopt a gender-integrated approach to data collection and analysis, because without data on the gender differences of outbreaks, trends and risks can be obscured, response management will be ineffective. Gender data is needed to understand the nuance of what is happening in the COVID-19 crisis and how gender dynamics may play out in various contextual settings.

OPPORTUNITIES

Closing the gender digital divide increases women's access to information. Digital technology enables access to critical health services and opportunities for education, civic participation, and economic engagement. It acts as a vital gateway for women to access information that can improve their livelihoods and significantly enhances their ability to contribute to their families and the global community.

Leverage the private sector and government focus on reaching last-mile populations through digital platforms. Consider how to work with mobile network operators, local Internet service providers, and other digital technology companies, such as app developers, to demonstrate the business case for inclusive connectivity and digital tools.

Resources and contact information

For more information on the gender digital divide, please contact digitaldevelopment@usaid.gov.

USAID
FROM THE AMERICAN PEOPLE

TRACK 2: HELP PARTNERS NAVIGATE RISK AND REWARDS: CONSIDERATIONS FOR COVID-19 RESPONSE

DIGITAL LITERACY

USAID's first-ever Digital Strategy outlines a path to strengthen open, inclusive, and secure digital ecosystems in all partner countries, and calls on the Agency to "increase our efforts to improve digital literacy of all people to advance development."

DIGITAL LITERACY IN THE CONTEXT OF COVID-19 AND DEVELOPMENT

In light of physical constraints and concerns due to COVID-19, many countries are proactively embracing and exploring new options for advancing access to digital tools and resources to support work, education, and the delivery of important healthcare information. Digital literacy training and skills are crucial to facilitating this transition and to longer-term human capital investments in a country.

USAID aims to ensure equitable access to digital literacy skills and training, particularly for marginalized populations including women, persons with disabilities, and other underrepresented groups. These groups should be supported with safe and responsible access to the Internet and other digital technologies to receive, share, and produce content.

WHAT IS DIGITAL LITERACY?

Digital literacy skills are those necessary to, "access, manage, understand, integrate, communicate, evaluate, and create information safely and appropriately through digital devices and networked technologies for participation in economic and social life." There are two pillars of digital literacy: capacity and safety. Capacity is the hard skills people need to access the Internet and utilize a variety of digital platforms including computers, mobile devices, and other media (e.g, audio and video). Safety encompasses the soft skills of using digital tools safely, including online security, privacy, and information and media literacy.

KEY CONSIDERATIONS FOR DIGITAL LITERACY IN COVID-19 RESPONSE PROGRAMMING

When designing digital literacy programs or working with external partners and stakeholders to implement digital literacy activities, please consider these guiding principles:

- **Strengthen the local ecosystem:** Support digital literacy and digital skills for digital employment/entrepreneurship by promoting local partners (civil society and private sector) that are already working to advance these skills. In doing so, be mindful of significant gender gaps in information, communications and technology (ICT) access and use, and work to overcome them.
- **Combat misinformation in health and COVID-19:** The importance of digital skills to distinguish between credible and accurate sources of news and information and misinformation.
- **Develop effective content:** Facilitate access to relevant digital literacy skills and training materials, promote local language digital literacy training materials, and support material development with locally relevant examples and case studies.
- **Accelerate innovative responses:** Those individuals with high digital literacy skills can design activities and produce new/re-tool digital apps (e.g, hackathons) that can support Covid-19 response, advocacy, and recovery efforts.

CONSIDERATIONS FOR COVID-19 RESPONSE
DIGITAL LITERACY

Questions to ask when designing a digital literacy program:

- Are you ensuring equitable access to digital literacy training, particularly to marginalized populations (e.g. women, persons with disabilities, rural communities)?
- Are you training and building upon existing infrastructure? For example, are you strengthening skills development that uses prevalent media (e.g., computers, Internet, mobile, audio, video)?

Questions to ask partners (private sector, governments, civil society and other stakeholders):

- How can digital literacy efforts better support your global/regional/national COVID-19 response?
- Is your activity duplicative and/or displacing the work of other institutions?
- Does your activity address and seek to overcome gaps in digital use and skills?

Similarly, there are risks and opportunities that can arise during a response to a global pandemic and need to be considered. Examples of risks and opportunities can include:

RISKS

The short-term digital literacy intervention inadvertently increases inequality and the digital divide, particularly among women and those with disabilities.

Immediate relevancy of your digital literacy intervention; digital literacy skills and training may not be accessible or important for short-term, as opposed to longer-term, response and recovery efforts.

OPPORTUNITIES

There is intense focus on the value and importance of using digital platforms in light of COVID-19 response and recovery to increase access to information which can help overcome physical distance challenges.

Forming deep, long-term partnerships and collaboration with a variety of organizations working in the global, national, and local digital literacy ecosystems.

Resources and contact information

For more information on digital literacy, please contact digitaldevelopment@usaid.gov.

USAID
FROM THE AMERICAN PEOPLE

TRACK 2: HELP PARTNERS NAVIGATE RISK AND REWARDS: CONSIDERATIONS FOR COVID-19 RESPONSE

CYBERSECURITY

USAID's first-ever Digital Strategy outlines a path to strengthen open, inclusive, and secure digital ecosystems in all partner countries, and calls on the Agency to "expand our capacity to help governments, the private sector, civil society, and citizens in partner countries to mitigate harm through cybersecurity programming."

CYBERSECURITY IMPLICATIONS FOR COVID-19 AND DEVELOPMENT

Cyber attacks on health systems, the media, civil society, small and medium size businesses, and development and humanitarian programs have significantly increased during the COVID-19 pandemic.[1] Tech firms have identified COVID-19 as the biggest topic ever used as bait for phishing attacks, with a near 700 percent increase in attacks since the pandemic started.[2]

Nation states and cybercriminals regularly use times of crisis to launch attacks, taking advantage of associated fear and confusion. Disinformation about the pandemic is prevalent and often includes hyperlinks used to spread malware and facilitate further hacking efforts. For example, in Ukraine violent protests broke out after hackers sought to sow public fear by spreading false information through a spoofed mass email that appeared to be from Ukraine's health ministry.[3]

The cybersecurity risks emerging during the global pandemic could both undermine response efforts and the long-term resilience and health of the digital ecosystem in developing countries.

CYBERSECURITY IN DEVELOPMENT

Cybersecurity for development can be understood as identifying, protecting, detecting, responding, and recovering from threats and risks in a digital environment. For USAID programs this includes the policies, regulations, processes, and technical standards for the security of programs operating in an online or digital world, and also the security and stability of the digital infrastructure and systems—in the places we work—that are critical to attaining development objectives.

KEY CONSIDERATIONS FOR CYBERSECURITY IN COVID-19 RESPONSE PROGRAMMING

Increased cyber threats require improved cybersecurity awareness across COVID-19 responses in all sectors and dedicated support to build the cyber capacity and resilience of our partner countries, institutions and citizens. When designing programs or working with external partners and stakeholders to implement COVID-19 response activities, these considerations can provide guidance.

Just as hand washing is critical to stopping the spread of the virus, the basics of cyber hygiene are now more important than ever and are the best place to start. There are practical steps that can help mitigate cyber risks in COVID-19 response programming.

- Have basic cyber hygiene practices been defined for programs and are they being followed by your implementing partners and beneficiaries?
- Are implementing partner and beneficiary staff now working from home? What measures have organizations taken to mitigate related threats?

1. https://www.devex.com/news/covid-19-brings-wave-of-cyberattacks-against-ngos-96934
2. https://www.bbc.com/news/technology-52319093
3. https://www.cnbc.com/2020/02/21/coronavirus-ukraine-protesters-attack-buses-carrying-china-evacuees.html

Practical steps that can help mitigate cyber risks in COVID-19 response programming (continued):

- If implementing partners or beneficiaries become the victim of a ransomware attack, do they have a planned response? Best practices for responding to cyber incidents can be found here.
- How would programs be affected if data was lost or compromised due to ransomware or other attack? Is critical data being regularly backed up and secured through multiple copies that are stored in separate virtual locations?

For these kinds of challenges, USAID has a new mechanism called Digital Apex, that is designed to help USAID partners and non-governmental beneficiaries improve their cybersecurity practices. Missions can also explore what capable and trusted local cybersecurity companies are available to help partners and beneficiaries prepare for and respond to cyber attacks.

IMMEDIATE RISKS:

Increasing **cyber threats have the potential to cause significant disruption** across sectors, further exacerbating the impacts of the COVID-19 crisis and limiting response efforts. What cybersecurity threats are happening in your country?

- Explore where you can learn about phishing, disinformation and misinformation trends occurring locally. Is there a local civil society organization, local cyber firm, or government ministry tracking cyberattacks and sharing information about risk? Can you access that information to share with partners and beneficiaries?
- Are the government's critical infrastructure systems, such as healthcare, financial services, communications (including Internet and social media), and energy, being hit with cyber attacks? If these systems were to shut down temporarily due to an attack, how would it affect programs?
- To the extent they exist, has there been an increase in public digital surveillance operations since the start of the pandemic? If so, how could it impact USAID programs or beneficiaries? What steps, if any, are beneficiaries or partners taking to mitigate concerns?

FUTURE RISKS:

Strengthening the cyber capacity and resilience of governments, civil society, private sector and citizens is crucial for supporting social and economic recovery over the coming years. These are some questions you can ask to better understand the cybersecurity landscape in your country and identify possible areas for programming:

- What is the capacity of the partner country to assess and address cybersecurity vulnerabilities of essential government services and critical infrastructure?
- What systems are in place to detect and deter cyber attacks in the organizations and institutions with which we are working?
- Is there an adequately skilled cybersecurity workforce?
- What are the basic levels of digital literacy and cyber security awareness of citizens?
- Has a partner country developed its own cybersecurity framework? Has it developed effective regulations to deal with cyberthreats?

OPPORTUNITIES

USAID programming can help address immediate cyber risks related to the pandemic and identify ways to engage host country governments and institutions to build cyber capacity and resilience. Talk with your host government counterparts to understand their cybersecurity needs and capabilities and identify where USAID can provide support.

USAID's Center for Digital Development has technical expertise available to help assess and design cybersecurity programming, and manages Digital Frontiers, a buy-in mechanism that works with USAID, the private sector, and international and local development organizations to identify successful and sustainable digital approaches and scale their impact globally.

Resources and contact information

For more information on cybersecurity, please contact digitaldevelopment@usaid.gov.

USAID
FROM THE AMERICAN PEOPLE

TRACK 2: HELP PARTNERS NAVIGATE RISK AND REWARDS: CONSIDERATIONS FOR COVID-19 RESPONSE

USING DATA RESPONSIBLY: PROMOTING DATA PRIVACY

USAID's first-ever Digital Strategy outlines a path to strengthen open, inclusive, and secure digital ecosystems in all partner countries, and calls on the Agency to "increase our investments in the privacy and protection of data in our programs."

USING DATA RESPONSIBLY: PROMOTING DATA PRIVACY IN COVID-19 AND DEVELOPMENT

USAID's approach to using data responsibly is to balance **use, privacy and security**, and **transparency and accountability**. First and foremost, we seek to **do no harm**. The framework recognizes the huge potential that data has while also recognizing that it comes with risks, especially for vulnerable individuals and groups. The Agency has developed **comprehensive policies and guidance** that adapt to keep pace with changing contexts, including ADS 508, ADS 545, and ADS 579.[1] USAID staff must follow these Agency policies in every aspect of decision-making, even in crisis situations.

Data privacy is the **right** of an individual or group to **maintain control over and confidentiality of information about themselves**. Data privacy can be at risk from both unintentional sharing, and from undue or illegal gathering and use of data about that individual or group. Through the *Digital Strategy*, USAID has committed to increasing investment in programmatic and ecosystem-level data privacy and protection.

Health data, a particularly sensitive type of personally identifiable information (PII), includes information on whether an individual has tested positive for COVID-19 and whether an individual is currently seeking treatment or hospitalized for COVID-19. There are ethical, legal, and policy issues to consider before making internal decisions or advising a host government, implementing partner, or international organization on the collection and use of sensitive data. For example, if a government identifies citizens who have been confirmed positive or potentially exposed to COVID-19, and publishes their home addresses or other identifying information, **it could lead to harassment and future threats such as job loss or penalties**. There is also risk that the data or mobile device applications may be used for purposes other than originally intended, which can have lasting implications on an individual's privacy or human rights. It is important to navigate legal and policy considerations with the General Counsel (GC) and your Resident Legal Officer (RLO).

KEY CONSIDERATIONS FOR USING DATA RESPONSIBLY IN COVID-19 RESPONSE PROGRAMMING

Responders and decision makers need accurate, timely, and reliable data to understand and prevent the spread of COVID-19 and citizens need access to accurate information to protect themselves. This critical need for timely data can lead some to make data privacy and protection an afterthought.

There are a lot of proposals to gather PII to, for example, track the spread of COVID-19, or to surveil individuals to ensure compliance with quarantines. These often use digital technology such as mobile phones to track location data, mine social media data, etc. There have also been several requests from our partner governments to our implementing partners to share sensitive information to help fight COVID-19.

1. This commitment to adhere to our policy laws and policies even during a pandemic is reiterated by OMB guidance and shared with the State Department guidance. https://www.whitehouse.gov/wp-content/uploads/2020/03/M-20-19.pdf

CONSIDERATIONS FOR COVID-19 RESPONSE
USING DATA RESPONSIBLY: PROMOTING DATA PRIVACY

Before moving forward, think through the benefits and risks of collecting/using/sharing data. You can conduct a benefit/risk analysis. For an example, see pg. 11 of the Considerations for Using Data Responsibly at USAID. You should also consult the **Fair Information Practice Principles (FIPPs)**, and other international principles that inform many privacy policies, including our own (see ADS 508).

Here are some questions to ask (within USAID and for partners, host countries, and other third parties) when considering such proposals, in coordination with GC or your RLO:

HOW WILL THE DATA BE **USED**?

- Who collected/will collect this data? Who **owns** it? Who has the usage rights and licenses?
- Is this data **necessary** - is there evidence that it will improve public health response? *If not, reconsider collecting it.*
- Is the **minimum** amount of data necessary for decision making being collected? *If not, reconsider exactly what data will be needed and minimize the data collected.*
- Is this data **representative** - is mobile phone/internet penetration high enough that the data will provide enough information? *If not, is there another set of data that will be more representative?*

WHO WILL THE DATA BE **SHARED** WITH?

- Who is it being **shared** with (and what data is being shared)? Can the data be transmitted/shared in a secured manner? Can the party receiving the data **protect** it?
- Is **relevant** data being **shared** with relevant stakeholders — partners, governments, donors, etc? *If not, why not?*
- What was the individual's expectation when their data was collected? Were they asked if their data could be shared outside of its intended use? Was **informed consent** obtained before collecting personal data? *This is a USAID requirement. Consult ADS 200mbe for USAID projects.*

HOW IS THE DATA BEING **PROTECTED**?

- Does the project have the necessary **resources** (information security tools, policies, and people) and are necessary **safeguards** in place to enable responsible collection, use, and management of data? *If not, what safeguards are appropriate (including de-identification, access controls, and other security/privacy requirements).*
- Where will the data be stored? How is data being **protected - now and in the future**? Will aggregating data (within a neighborhood, city, etc.) protect individual privacy while maintaining its usability? Will vulnerable populations still be identifiable? Demographically identifiable information (DII) could exacerbate misinformation about specific communities if COVID-19 related data shows some communities are disproportionately affected. *Consult ADS 545.*
- What are the **implications of loss of privacy**?
- What are the **plans** in the event of a data breach?
- What **laws** are currently in place in the country that relate to data privacy or user rights? Have you consulted with appropriate authorities (including local counsel) to ensure the proposed use complies with relevant laws and policies? How else are you promoting compliance?

RISKS AND OPPORTUNITIES

Loss of privacy can hurt individuals (risk of physical harm, restriction of movement/freedom by the state or other actors), organizations (reputational harm), and have a detrimental effect on USAID programming. Protecting individuals' privacy increases trust in institutions, both public and private. Building trust in systems encourages use, which increases accuracy, validity, and usefulness of data. It helps organizations and governments allocate resources for informed decision making. It also increases our ability to provide services to the people who we serve.

Resources and contact information

For more information on data privacy, please contact digitaldevelopment@usaid.gov.

USAID
FROM THE AMERICAN PEOPLE

TRACK 3: SHIFT TO DIGITAL BY DEFAULT: CONSIDERATIONS FOR COVID-19 RESPONSE

HOW TO RESPONSIBLY INVEST IN DIGITAL TECHNOLOGY

USAID's first ever Digital Strategy outlines a path to strengthen open, inclusive, and secure digital ecosystems in all partner countries, and calls on the Agency to "mandate the digital collection of programmatic data."

As the world responds to COVID-19, local institutions are receiving proposals intended to address challenges in health, education, and social services. The concepts often include technology, and range from simple to complex.

Digital tools are central to the COVID-19 response. Responders need detailed and timely data to understand and prevent the spread of the disease, and communities need access to accurate information in order to protect their families. Children are using digital technology to learn, people are using digital payments to send money to loved ones, and local institutions are entering the online space to deliver services that have been impacted by the epidemic. This requires strong digital tools, policies, and infrastructure to support the responsible use of technology and address inequalities.

YOU MAY BE ASKING:

- Should we fund an AI-based predictive disease modelling system?
- Should we pivot our programming to train educators through YouTube?
- Should we partner with the private sector to set up a call center for social services?
- Should we support the government to roll-out an app that ensures citizen compliance with quarantine orders?
- How can we expand our radio programming to address COVID-19?
- Is it worth piloting an e-Learning tool to support local education during COVID-19?

Here are **eight topics** to consider when assessing a proposal that includes a digital intervention. These tips are built on extensive USAID tools: the Digital Investment Tool, the Digital Health Investment Review Tool, and on lessons learned during the Ebola response. These are intended to support Missions, partners, and host country institutions to identify investments that achieve positive development outcomes.

1. START WITH THE DEVELOPMENT CHALLENGE: What is the specific local COVID-19 challenge we are trying to solve? Is a digital intervention beneficial? Ensure this is not a "solution" searching for a problem.

2. ENSURE LOCAL OWNERSHIP & ENGAGE WITH RELEVANT STAKEHOLDERS: Is it important for host-country institutions to be able to manage the digital intervention? Would your intervention inadvertently displace the efforts of local actors? Building upon existing initiatives, using tools that are locally maintained, and incorporating local vendors, will lead to a greater chance of the system being used during and after the activity.

3 ASSESS THE LANDSCAPE AND REUSE AND IMPROVE: Is the digital intervention relevant to the local context? For example, if a digital tool requires data to be shared, but only 20% of clinics have connectivity, it may not be the best choice. Can the proposal be modified to reuse existing platforms that are already in place? How can local laws and protocols on technology and data be accomodated? Proposals that introduce new solutions need to reflect what's possible in the local context.

4 DESIGN WITH THE USER: How will users be consulted during the design process (ex. features, content, governance) when social distancing is emphasized? How can the system be adapted around users, rather than forcing users to accommodate (ex. what are users' existing media and communication preferences)? In an emergency, digital tools that are not intuitive will not be effective.

5 ENSURE DATA PRIVACY & SECURITY: How are we protecting data, especially sensitive data, during the response to COVID-19? Who owns and has access to the data being collected? Privacy is a right and protecting it can ensure trust. Consider potential privacy and security risks and mitigation efforts at every point in the data management lifecycle.

6 IS THE TOTAL COST OF OWNERSHIP REALISTIC? Does the system need to be affordable to local stakeholders? Does the budget include all necessary costs for the activity to quickly and successfully deploy to address COVID-19 (ex. system configuration, deployment, training, user testing, transaction, service, and licensing fees)? A resource mobilization plan can help activities last beyond donor funding.

7 WILL IT SUSTAIN OR SCALE? Could collaboration with local institutions, donors, and the private sector increase the possibility of scaling during and after the response to COVID-19? Many digital interventions don't survive past their pilot period. Defining a pathway to scale and ensure sustainability from the beginning can help an activity succeed.

8 IS IT OPEN AND INTEROPERABLE? Do current conditions warrant an open-source license, such an Open Data Commons or Creative Commons license? Is it important for the proposed solution to be interoperable with other locally used systems? During the Ebola response, siloed systems led to a fog of information that was difficult to see through.

OPPORTUNITIES

USAID programming can help support host country institutions assess technology proposals related to COVID-19 response and recovery. Speak with your counterparts to understand their technology procurement needs and capabilities and identify where USAID can provide support. USAID has additional mechanisms and technical support available for Missions. Please contact us for a consultation.

Resources and contact information

For more information on digital best practices, or to schedule a consultation on the Digital Investment Tool, please contact digitaldevelopment@usaid.gov.

USAID
FROM THE AMERICAN PEOPLE

TRACK 3: SHIFT TO DIGITAL BY DEFAULT: CONSIDERATIONS FOR COVID-19 RESPONSE

DIGITAL DATA COLLECTION

USAID's first ever Digital Strategy outlines a path to strengthen open, inclusive, and secure digital ecosystems in all partner countries, and calls on the Agency to "mandate the digital collection of programmatic data."

DIGITAL DATA COLLECTION IN THE CONTEXT OF COVID-19 AND DEVELOPMENT

Information is critical to fight the spread of COVID-19. Responders and decision makers need detailed and timely data to understand and prevent the spread of the disease. Health workers and communities need access to accurate information to protect themselves and their loved ones. Governments need to understand how their policies to respond to COVID-19 are affecting citizens. USAID Mission staff and Implementing Partners need to continue to monitor their programs remotely and assess how digital data collection tools can be adapted to support continued monitoring of programs and collect data relevant to COVID-19 response efforts.

WHAT IS DIGITAL DATA COLLECTION?

USAID's *Digital Strategy* recommends that Agency staff and partners collect programmatic data digitally (e.g. by tablet, mobile phone, etc.) rather than paper to the greatest extent possible.[1] Ultimately, the goal is to use the data collected for better decision-making, adaptive programming, and strategic planning.

KEY CONSIDERATIONS FOR DIGITAL DATA COLLECTION IN COVID-19 RESPONSE

Questions to ask when discussing digital data collection:

- **What information do you need, and who has it?** Knowing the type of information you need and who can provide it will help to narrow the choice of which digital data collection tool to use. For example, if you need information from groups that may have low literacy, interactive voice response or phone surveys may work best.
- **Is someone already collecting this information?** Only collect new data after identifying existing datasets and ongoing data collection to ensure you are not duplicating efforts. Consider identifying a data "czar" to coordinate data analysis and share across agencies, coordination groups, host country governments, etc.
- **What digital data collection tools have been deployed in my area of interest by USAID partners or other groups?** Does your Mission have a monitoring, evaluation and learning (MEL) mechanism that has experience with digital data collection? How are implementing partners collecting their data? Consider adapting and expanding systems that are already in use before developing any new digital data collection efforts.
- **Can you reach your population of interest by SMS, phone or Internet? If not, are there key informants** (e.g., field-based project staff, extension workers, community health workers, non-governmental organizations, etc.) **that can be reached by SMS, voice calls or mobile apps to support data collection?**

1. USAID will make exceptions to this mandate on a case-by-case basis.

Questions to ask partners - private sector, governments, civil society and other stakeholders:

- **What assets outside of USAID's network can be leveraged?** For example, are there private sector call centers that can be used to conduct computer assisted telephone interviews (CATI)?
- **What data collection systems are already in place by market research firms, civil society and host country governments? What data are these other stakeholders collecting?** Develop data sharing agreements where appropriate.

Similarly, there are risks and opportunities that can arise during a response to a global pandemic and need to be considered. Examples related to digital data collection can include:

RISKS

Nearly all digital data collection tools that can be used remotely require mobile or Internet connectivity. Some populations without access could be omitted, resulting in biased data. Consider using key informants in different communities to collect data to mitigate this issue.

In countries where mobile phone ownership and Internet use is lower among women than men, consider how this gender disparity will affect any digital data collection efforts.

Data collection and data sharing has inherent risks to privacy. See more on data privacy.

OPPORTUNITIES

Using digital tools to continue USAID's data collection efforts to overcome physical distance challenges brought about by COVID-19 for both information gathering and activity monitoring.

Coordinating between different stakeholders to develop a strong data ecosystem can help decision-making by USAID and our partners during the COVID-19 crisis and beyond.

Resources and contact information

For more information on digital data collection, please contact digitaldevelopment@usaid.gov.

USAID
FROM THE AMERICAN PEOPLE

TRACK 3: SHIFT TO DIGITAL BY DEFAULT: CONSIDERATIONS FOR COVID-19 RESPONSE

DIGITAL PAYMENTS

USAID's first-ever Digital Strategy outlines a path to strengthen open, inclusive, and secure digital ecosystems in all partner countries, and calls on the Agency to "make digital payments the default method of payment under all our awards."

WHAT ARE DIGITAL PAYMENTS?

Digital payments are transfers of money enabled by, or delivered through, digital technology. For example, digital payments can be made through mobile money, mobile wallets, digital bank accounts, QR codes, credit/debit cards, or online payments. Under the right conditions, digital payments offer benefits over cash: they are faster, cheaper[1], more convenient to use and process, more secure, can build a user's financial profile, and can be a foundation for other financial services (savings, credit, insurance, etc.).

Alongside other methods for cash-transfer programs, digital payment channels can support more rapid, transparent, cost-effective distribution of funds as long as certain factors are accounted for, including: mechanisms for enrollment, agent-level cash-out, and merchant-level digital payments (so recipients can avoid reverting to cash).

DIGITAL PAYMENTS IN THE CONTEXT OF COVID-19 AND DEVELOPMENT

Broadly, digital payments have factored into COVID-19 responses in two primary areas. The first area is social safety net programming. While often managed by NGOs, the largest of these programs involve Government-to-Person (G2P) payments to individuals and households impacted by the crisis, particularly the poorest and most vulnerable who are being disproportionately affected. As of July 10:

- A total of 200 countries and territories have planned or put in place 1,055 social protection measures in response to COVID-19. Social assistance accounts for 60% of the social protection response or 638 measures.
- With 298 cash transfer programs in 139 countries (6 of which are universal transfers), cash-based transfers account for nearly half of those safety net measures, and about 30% of global measures.
- The size of cash transfers more than doubled in five countries (Mongolia, Trinidad and Tobago, Egypt, South Korea and Brazil). Overall, transfers represent 29% of average monthly GDP per capita.
- Using the sole metric of horizontal coverage expansion for cash transfers, then such scale-up covered almost 1.1 billion people or 14% of the world's population.[2]

1. Because the payment is done digitally, there's no need to hire people to make the transfer manually, recipients don't need to wait in line to receive their payment thus saving the monetary value of their time, there is more transparency and therefore less costly corruption ("losses") and bribes that can happen, etc.
2. World Bank, "Social Protection and Jobs Responses to COVID-19: A Real-Time Review of Country Measures," July 10, 2020, World Bank Group, http://documents1.worldbank.org/curated/en/454671594649637530/pdf/Social-Protection-and-Jobs-Responses-to-COVID-19-A-Real-Time-Review-of-Country-Measures.pdf

The second major area that digital payments factor into is operational support. Here, as shown by the Ebola crisis, digital channels can ensure continued payments to health workers, contact tracers and frontline workers, often operating in informal settings with no access to a bank account or even a national ID.

Despite widespread efforts by governments to utilize digital payment platforms, countries may face a number of challenges and risks. Below is a chart of emerging issues in deploying responsible payments in response to COVID-19, and where USAID Missions can focus their effort. Among the issues and mitigation approaches listed below, it's important to consider taking a gender intentional approach to each.

ISSUE	MITIGATION APPROACH
TARGETING - Whom do you include that is not already receiving social benefits?	Engage local leaders, private sector service providers, and influencers to assist in product design and enrollment programs that target individuals that have the greatest need. Support peer exchanges between governments and experts from different regions who have successfully targeted vulnerable households in their respective countries.
ONBOARDING - How do you rapidly onboard a large number of low income and rural people onto digital platforms to receive payments?	Assist governments with implementing appropriately relaxed regulatory measures that may include adoption of tiered Know-Your-Customer (KYC) policies or developing legal frameworks to enable both bank and non-bank providers to offer basic transaction accounts that are plugged into formal payments infrastructure.
LIQUIDITY - How do you ensure sufficient, reliable financial liquidity in the financial sector and at cash-in/ cash-out points?	With the deployment of social benefit transfers or salary payments, recipients will need to either cash out or purchase goods and services digitally. This requires sufficient cash within agent networks or merchant acceptance of digital payments. Facilitate dialogue between governments and the private sector to identify policies or programming that facilitate the safe mobilization of agent networks or introduce solutions that promote merchant acceptance of digital payments and Person-to-Person (P2P) transactions. Help support country mapping of financial access points to analyze distribution and explore different incentive / subsidy models that ensure the viability of Cash-In-Cash-Out (CICO) points.
EXCLUSION - Is the intervention inclusive of marginalized populations? Gender, age, social groups, race, etc.? What does that mean in terms of access? Does the end user understand digital products and would they be willing to use it over cash?	Advise governments on the use of multiple data sources that can ensure targeting is inclusive. Assist in developing monitoring systems that track benefits and use among marginalized populations. Ensure that providers have processes and resources that ensure all beneficiaries are treated appropriately. Work with providers to prioritize women and other underrepresented populations in workforce development, both at the corporate, merchant, and agent level. Ensure gender sensitivity and inclusion is embedded in all aspects of these trainings. Support digital readiness programming that ensures customers understand the benefits and responsible use of digitally enabled financial services and don't fall prey to fraud or errors.
MONITORING - How can you monitor programs to make sure they are working effectively? How do you diagnose issues?	Support digital monitoring systems that communicate with intended beneficiaries or frontline workers to identify issues early and often. Ensure there's a system in place, such as a centralized "help center" for effective recourse and to minimize cases of fraud.

Resources and contact information

For more information on digital payments, please contact digitaldevelopment@usaid.gov.