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.

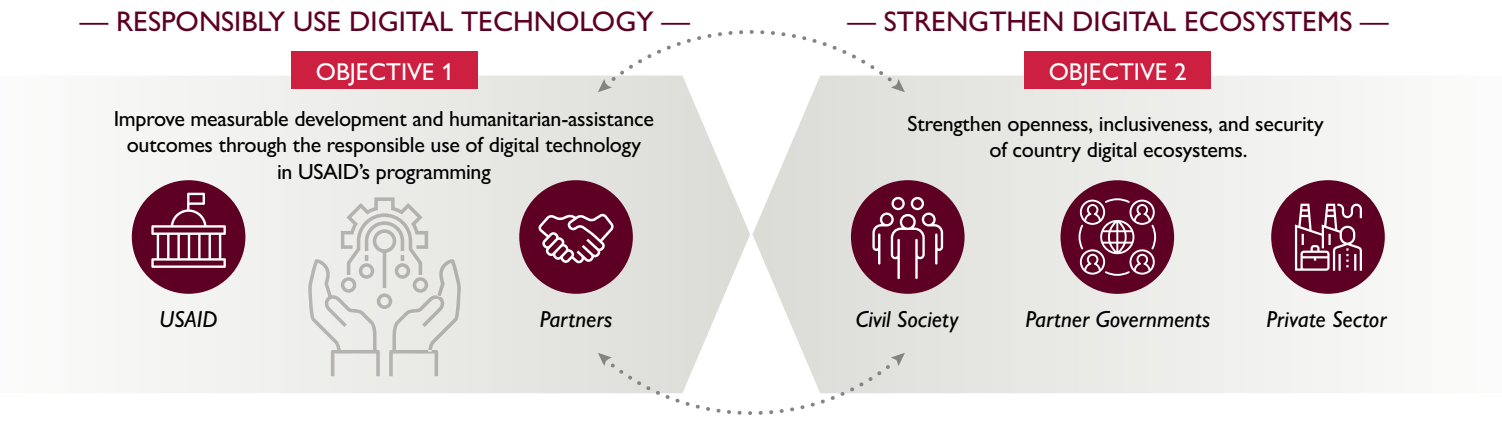
THE DIGITAL REVOLUTION has given way to the promise of a digital world that spurs economic growth, improves health outcomes, and lifts millions out of poverty using new technologies and services. While digital tools present immense potential to advance freedom and transparency, generate shared prosperity, 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

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.