USAID Bureau for Humanitarian Assistance
Emergency Application Guidelines

Draft Data Management Approach Guidance

Data Protection and Privacy

Per USAID’s “Considerations for Using Data Responsibly at USAID,” data constitute recorded information, regardless of form or the media on which the data may be recorded. The term includes technical data and computer software. For the purposes of this section, BHA is concerned with all data collected from or about beneficiaries and others in the community of the planned activity, including, but not limited to, beneficiary personally identifiable information (PII), health records, biometrics, geospatial information, and group demographics. Please ensure that you have a clear understanding of key data concepts such as Open Data, Data Aggregation, PII, and sensitive information as described in the “Considerations for Using Data Responsibly at USAID,” and that any proposed use of data within your application reflects that guidance. (NOTE: links to new IASC framework and ADS 579: USAID Data Policy will be added, once they are established, approximately June/July 2020.)

Responsible data management throughout the program cycle must take into consideration what information needs to be collected, what it will be used for, and who will have access to it. The activity may only collect information that is directly pertinent to successful implementation and learning opportunities, such as variables used to determine eligibility and measurements of outputs and outcomes. You should avoid the collection of non-essential PII. When it is necessary to collect PII, you must put into place procedures including appropriate delivery of informed consent to ensure that individuals have a clear understanding of the limits on usage of the data. You must include sufficient budget in your application to cover costs of responsible data management and protection.

USAID expects all partners, including any third parties, to have strong data protection protocols that are followed consistently and are adequate to protect all collected data. You must collect, process, and manage data in accordance with local laws and regulations and are encouraged to follow the principles outlined in the Principles for Digital Development and EU’s General Data Protection Regulation (GDPR). Any breaches of data privacy and security must be reported immediately. Please consult with your AOR regarding required reporting.
Data Collection and Beneficiary Consent

When requesting consent to collect and use beneficiary data, you must explain the steps you will take to obtain informed consent from beneficiaries. Include in your description how you will convey that the information will be maintained in a confidential manner to protect beneficiaries and that their participation is voluntary. You must inform beneficiaries of any other organizations with which their data may be shared, such as other humanitarian organizations and government ministries. You must also inform beneficiaries of all potential uses of their data, including direct programmatic use, integration into broader analysis and visualization, and use in new technology approaches, such as machine learning and artificial intelligence.

You must disclose to beneficiaries the potential risks and consequences they could face by consenting or not consenting to providing their personal information. Possible risks and consequences may range from the denial of humanitarian assistance or services, to exposure of data to unauthorized entities and data misuse.

You must inform beneficiaries how they can file a complaint or concern with regard to the collection and handling of personal information, linking them to the complaint and response mechanisms in place per the Accountability to Affected Populations requirements described in Section 10.6 of the BHA Emergency Application Guidelines.

Invasive data collection methods, such as biometric technology, present greater risks. When choosing to use or implement biometric technology:

- You must document and justify the need for a biometric solution by specific use for this type of solution. This includes choices on configuration, biometric data processing, the scale of implementation, and the holding of the biometric template (data storage).
- You must explain your measures to mitigate risk and fortify security of the biometric scanning device and data storage.
- You must ensure that Individuals’ unique identities and biometric impressions never leave the local device or be transmitted. BHA authorizes machines to transmit only biometric validations outside the local cache, never the biometric impressions themselves.

Data Management

You must describe your system for data governance, including roles and responsibilities of personnel who control and manage data assets and the policies and procedures in place to protect the management, use, and storage of programmatic and beneficiary data assets. Include an overview of your organization's practices for managing the lifecycle of data and information as it relates to security and privacy, including retention, frequency of access, processing, storing, aggregating, transmitting, and erasure. You must tag beneficiary personal data when information is collected, processed, and amended throughout the program or activity lifecycle. Systems must enable access and have the capacity to correct data as necessary.
Your compliance with data protection and privacy principles must be demonstrated through adequate training, monitoring, and auditing.

**Data Access**

Proper data access and account management is crucial to ensuring data are controlled and accessed by qualified persons on a need-to-know basis. You must describe your policies and procedures to establish and maintain control over user access to information systems and paper-based documentation. It is recommended that data access is governed by role-based and policy-driven administration, as well as procedural and technical controls.

**Internal Permissions, Access, and Controls**

You must establish and maintain effective account administration and governance to protect the integrity of data and the user identity repository of all individuals who are authorized to interact with the data and managing system. You must describe internal policies and governance to effectively manage users for both digital and paper-based systems. Examples of effective data management include:

- Measures that will be taken to track and secure every user and account type including individual, shared, and administrative accounts, such as root and local administrator.
- Processes for information collection from your internal teams and divisions to effectively track, monitor, and make relevant changes to user access.
- Internal policies to prevent and detect unauthorized data access for data entry, editing, processing, or retrieval.
- Security measures to protect physical and virtual data assets, including location of hard copies, databases, virus protection, and data backups.

**Third Parties**

Awardees often depend on third-party relationships to enhance the effectiveness and efficiency of humanitarian interventions. However, as outsourcing, contracting, and reliance on third-party services increases, so do the risks involved. If data are shared with or transferred to third parties in academia or the private sector, you must specify the nature and purpose of the relationship through appropriate and lawful contractual arrangements, agreements, or memorandums of understanding (MOUs). You must not share or grant access to sensitive data with third parties in the absence of an official agreement.

You must describe third party security controls and any measures to mitigate inherent privacy and security risks of exposing data to third parties, including the generation of metadata or automatic collection of personal data that could be sold or misused by third parties without your knowledge.

Agreements must establish how data will be shared and protected, and must include terms and conditions that safeguard personal data, program data, and its metadata (such as locality or
time and frequency of beneficiary interactions with the awardee) against potential misuse. You must ensure the ownership of data assets remain with your organization. Third party violations in the privacy and protection of beneficiary personal data should be addressed and remediated immediately. **BHA must be notified of any breaches in data privacy and security immediately.** Consult your AOR regarding required reporting.

**Data Sharing Agreements with Partners**

Data sharing agreements are intended for circumstances when you want to share data with a partner through a common database that is accessed through Application Program Interfaces (APIs). Information sharing enables you to co-coordinate and plan humanitarian activities based on a collective knowledge of needs, thereby strengthening programming and humanitarian coordination. BHA recognizes the positive impacts of data sharing, and supports accessibility and availability of relevant data among partners and the adequate systems infrastructure for their secure exchange and transmission.

Data sharing among partners should be governed by lawful agreements or MOUs and reflect best practices and incorporate ethical practices for data governance, security, and protection. You must describe your data sharing policies, your objectives for information sharing, and the rights granted to the operator, contributors, and users. Include specification of data elements and categories to be shared and the process for sharing various categories, including personal vs. non-personal data.

Careful consideration of the Application Program Interface (API) architecture and design is required and must be outlined in detail under the technical terms of the agreement or MoU. You must describe the processes in place for API management and security, including your identity and access controls. Include your process for granting levels of access and managing who has access to your APIs and when and how often they are used. Your API platform solution should include an API gateway and interoperate with your existing security architecture and access management infrastructure to avoid creating new silos of users. Your application must also include plans for ongoing maintenance, auditing, monitoring, and tracking of the API architecture and usage to ensure vulnerabilities are addressed and necessary updates are made in a timely manner. The Data Management Plan should be described in your Monitoring Plan Narrative (see Section 10.7 of the BHA Emergency Application Guidelines).

Shared data and files must be in machine-readable, encrypted format and transferred electronically through secured digital channels such as Secure Shell File Transfer Protocol (SFTP).

**Data Usage and Emerging Technologies**

Data and your ability to make use of the information effectively will enable you to make more informed decisions that result in successful program outcomes. BHA supports traditional and
novel approaches to data usage and analysis that are accountable, ethical, and enhance programmatic value.

If artificial intelligence (AI), machine learning (ML), or emerging technologies are leveraged to achieve program objectives, you must describe the use case, its link to programmatic value, and how its use is sustainable, secure, ethical, and driven by program outcomes. Your activity must be designed and implemented responsibly, employ the do no harm principle, and be guarded by a strategic plan with measurable and realizable goals. You are required to weigh the potential benefits against associated risks in AI and ML in your activity, including bias, unrepresentative or inaccurate data, discrimination, and/or flawed results that may cause harm to vulnerable populations. Decisions must not be generated by AI or ML results without evidence of the accuracy, effectiveness, and fitness for meeting the program objectives. You may participate in a model Peer Review Framework by submitting your predictive models for review and verification to the Predictive Analytics Team at OCHA’s Centre for Humanitarian Data.