MEETING TARGETS AND MAINTAINING EPIDEMIC CONTROL (EPIC) PROJECT

COOPERATIVE AGREEMENT NO. 7200AA19CA00002

Ensuring Compliance with the EpiC Data Safety and Security Checklist

APRIL 2021

PEPFAR

USAID FROM THE AMERICAN PEOPLE

EpiC Meeting Targets and Maintaining Epidemic Control

This resource was originally developed in 2020 with the generous support of the American people through the U.S. Agency for International Development (USAID) and the U.S. President's Emergency Plan for AIDS Relief (PEPFAR) through the LINKAGES project (#AID-OAA-A-14-00045). It was updated in April 2021 through the USAID- and PEPFAR-supported Meeting Targets and Maintaining Epidemic Control (EpiC) project.

The contents are the responsibility of the EpiC project and do not necessarily reflect the view of USAID, PEPFAR, or the United States Government. EpiC is a global cooperative agreement (7200AA19CA00002) led by FHI 360 with core partners Right to Care, Palladium International, Population Services International (PSI), and Gobee Group.

Foreword

HIV service delivery programs must "do no harm" for both their project staff and program beneficiaries. The safe management of project data—which often contains highly sensitive individual beneficiary and community information—is part of that duty. To support implementing partners in the safe management of project data, the USAID- and PEPFAR-funded Linkages across the Continuum of HIV Services for Key Populations Affected by HIV (LINKAGES) project developed an electronic Data Safety and Security Checklist designed to be used with the tips contained in this document. Both documents have been revised under the EpiC project. We offer these tools as working documents that can be downloaded and used to assist HIV program implementers—especially those working with members of key populations: gay men and other men who have sex with men, people who inject drugs, sex workers, and transgender people—as they implement safe and high-quality programs.

Introduction

Data safety is vital for the protection of individual service users and project staff and for the integrity of the project. The confidentiality of service users is of paramount importance, both ethically and for the implementation of effective programs. Breaches in service user confidentiality can lead to blackmail, physical and/or sexual violence, job loss, loss of custody of children, and the widespread marginalization of service users, as well as a loss of trust in health care services that negatively affects service uptake. Breaches in data safety can harm implementers who are targeted for their involvement in service provision. For the project, a failure to protect data can result in an inability to provide appropriate services or report on activities. To protect service users' data, implementer safety, and programmatic integrity, LINKAGES developed a list of actions that should be taken by implementing partners (IPs) collecting, managing, analyzing, and storing such data, referred to as the EpiC Data Safety and Security Checklist. It has been revised for the EpiC project and other HIV service delivery programs. Implementing partners and strategic information (SI) backstops should use the checklist and this more detailed guidance on implementation to ensure adequate protective measures are in place.

Please note: The checklist and this guidance document support data safety and security for HIV programs using paper and electronic data collection tools and databases. It does not cover the full range of communications (such as text, dating apps, or other messaging platforms) transmitted and stored on online and mobile platforms such as Facebook or dating websites. Guidance for data safety in online HIV programming can be found in the QuickRes Technical Guide, pages 9-11, or the LINKAGES's Vision for Going Online, pages 37-44.

The left column includes the checklist item from the EpiC Data Safety and Security Checklist and additional information on how to operationalize that item. The right column includes example documents (or elements of such documents) to support operationalization. It also includes illustrative language in italics to help populate those documents. **Illustrative language is meant only to help IPs think about the content of the documents and is not meant to be prescriptive.**

Section 1. Paper Records

Instructions	Documents to support operationalization (with illustrative examples)
1. Does the implementing partner have a list of all documents that require safe storage (i.e., all documents containing information that can be used to identify individual KP members)? • Update the list of documents each quarter when developing quarterly reports (in this process you may realize that you are using new documents that contain identifying information). • Include anything that contains individual level data with personal information about a service user.	List of documents requiring safe storage with date of last review • *Sign-in sheets* • *Clinical records* • *Outreach logs* • *Individual tracking data being used for microplanning*
2. Is there a space, such as a locked safe or cabinet, where paper records with individual identifying information are safely stored? • Storage space should be easily identifiable and during a site visit (if audited via visit), location should be checked to ensure that it is locked, and key is not easily found. • Have a mechanism in place to ensure duplicate keys cannot be made.	Description of safe storage location and protections in place • *File cabinet with lock* • *Only select staff have access to key, which cannot be duplicated*
3. Is access to the space for safe storage controlled by selected staff and monitored? • A list of staff who can access safely stored documents is kept with the list of documents that require safe storage. The list is updated whenever staff who have access stop working for the IP for any reason and should be reviewed quarterly. • Each time a staff member with access leaves the organization, the code (if a combination) is changed, and all keys are accounted for or locks are changed. • Someone in a position with relatively low turnover, such as the nongovernmental organization (NGO) director, should be the final person responsible for data safety. He or she will be referred to as the Data Safety Point of Contact and must be aware of and sign off on these changes when they occur. The Data Safety Point of Contact will also need to be trained (see section 4 below). • Add a logbook to track persons who have accessed the safe storage location at various times.	Names of staff with access to paper-based data and date of last review • *Staff name, date access began, date ended* • *Date of last review* Named Data Safety Point of Contact Logbook which tracks access to safe storage location

4. Does the implementing partner have guidelines and protocols for handling individual records, including a list of staff responsible for moving data to safe storage? • An easy-to-use graphic depicts data movement (e.g., from peer educators to data entry personnel) and names each individual and their position; it refers to protocols for safe handling of individual records. • Each job description for positions that entail data handling contains specific responsibilities around data storage and record handling, including a confidentiality clause. • A confidentiality statement should be signed by all those named as having access to identifiable data, including paper- and electronic-based. An example of a confidentiality statement can be found in the Program Monitoring Guide (p. 22). These must be safely stored so they can be referred to as needed. • Staff responsible for data entry (i.e., when paper-based data is entered into an electronic format), such as a monitoring and evaluation (M&E) officer, should also be named and sign the confidentiality statement.	Graphic describing how data circulates within the organization and program List of job descriptions that include safe data storage and record handling practices • *Peer outreach worker* • *Peer navigator* • *Drop-in center (DIC) manager* • *Monitoring and evaluation (M&E officer)* List of staff responsible for moving data with date that each person signed confidentiality agreement

Section 2. Electronic Data Systems

Instructions	**Documents to support operationalization (with illustrative examples)**
5. Are all databases password protected? • Computers require passwords to open them; databases should require an additional, separate password. Ideally, there will also be an administrative access password separate from the user's password. • A strong password will be around 10 characters or more and, where possible, always include upper-case letters, lower-case letters, numbers, and symbols.[1] Do not write down passwords to share them. • Passwords should be changed every three months, with additional changes if security has been compromised or with staff departure. • Systems to prevent sharing of passwords should be in place (two people should not have the same log-in credentials).	Log to track that all computers have passwords, and all databases have passwords Date that passwords were last changed on computers where data is stored Date that passwords were last changed on databases

[1]HeartMob. Technical Safety Guide [Internet]. Hollaback! c2020 [cited 2019]. Available from: https://iheartmob.org/resources/tech.

6. Is access to passwords for databases and electronic data controlled? • Any data containing identifying information must be in a password-protected file, including when sent by email or uploaded to the Cloud. • Describe who can access the database to enter data and to see the full database. Two different passwords (one for admin and one for other users) are required for access to the full database versus data entry.	Names of staff with access to electronic data and dates that access began and ended
7. Are unique identifier codes (UICs) or masking used instead of other identifying information such as client name? • The process of developing UICs should follow the Program Monitoring Guide (p. 23). • If using client facing databases such as ORA/QuickRes that collect personally identifying information such as client name and phone number, ensure that the systems are set up to "mask" any personally identifying information.	UIC generation guidance ORA and QuickRes are client management tools that anonymize client phone numbers on data exports and hide client phone numbers on the program-facing interface and can be revealed only individually to those with appropriate levels of access.
8. Are electronic data securely backed up and stored either in the Cloud and/or on an external drive in a remote location outside of the implementing partner offices? • The IP should decide on whether to use Cloud or local storage based on local guidance from government and the cost of Cloud storage (which will depend on the size of data to be stored). • Safe Cloud storage requires a password. If possible, use an encrypted storage platform such as Google Drive. • A portable backup storage device (e.g., a CD or USB drive) should also be password protected, and its location known only to those who have access to the full database. • Data must be backed up weekly. • Have a description of protections for backed-up data.	Describe backup • *Cloud* • *USB drive* • *CD* • *Date of last backup* Describe data protection • *Password* • *Encryption* • *Safe location of hard drive* *ORA or QuickRes systems are encrypted and backed up using a secured and trusted third party backup service.*
9. Does the implementing partner have a protocol for changing passwords when staff depart? • Each time a staff member with access leaves the organization, the password must be immediately changed. If the staff person is being terminated, the password should be changed before the decision to terminate is communicated to them. • If a staff member is changing positions within the organization and will no longer have access to the database, the password must also be changed immediately.	Illustrative language: *Whenever a staff member, consultant, or other individual with access to stored data or the ability to enter data is fired or leaves the organization, his or her access will be terminated. If he or she has a log-in name, the name will be deleted. In the case of firing, access to data will be stopped before the decision is communicated to the employee.*

10. Is the implementing partner's database hosted on a secure web server? • Whenever using an external cloud space to store data, the project should ensure that the web server is secured and has all the necessary security arrangements. Extra care should be taken if real time data collection is employed (e.g., DHIS2 tracker for individuals). • Software used for cloud-based databases should automatically allow for encryption of data during transmission. DHIS2 meets this requirement. • ORA or QuickRes systems use SSL encryption and the server host is secured according to the highest global standards.	Describe server protections in place, for example: ○ *Use of a secure file transfer protocol (FTP) instead of plain FTP* ○ *Use of a secure shell (SSH) instead of telnet* ○ *Securing all web administration areas with secure sockets layer (SSL) (HTTPS)* ○ *Securing your web forms with SSL (HTTPS)* ○ *Use of firewalls on all endpoints, including servers and desktops*
11. Is the implementing partner's database-hosting software updated whenever a new version or patches become available? • Particularly if the project uses real time data entry, make a provision for updating the system whenever a new version is available. Updates help execute new features of the software, including security protections. • Software updates often include patches. However, a stand-alone patch (or patches) may be released to fix critical security errors. These should also be employed immediately to avoid vulnerabilities.	Documentation can include a comparison of the current version of the software to the most recently released version. The database and site components of ORA or QuickRes systems that use the developer AD Systems Asia are updated automatically whenever a new version or patch becomes available. If you use another developer/IT vendor, check if they comply with these standards.
12. Is electronic data storage aligned with national standards? • National policies may include guidelines on the types of client data that can be stored electronically. For instance, some countries prohibit the storage of individual health data on servers outside their country. It is important for programs to be in line with, or exceed, such standards.	Review documentation on national standards and policies for the storage, updating, and maintenance of personal data.

Section 3. Data Sharing and Destruction Procedures

Instructions	Documents to support operationalization (with illustrative examples)
13. Does the implementing partner have protocols/guidelines for sharing data? This protocol should provide guidance on the two types of data sharing that occur. • Type 1: sharing for analysis and reporting ○ When sharing information to individuals who are outside the project and/or who will not be providing services, identifying information should not be shared. This includes the service user's name, address, and telephone number. ○ Information that is disaggregated should not be disaggregated to the point where individuals could be identifiable. Locations of KP members as a group should also not be shared. Sharing hot spot maps, even without street names, should not be done. More guidance specific to hot spot mapping and size estimation data collection and handling can be found in Mapping and Size Estimates of Sex Workers: Proceed with Extreme Caution. ○ The process for requesting data and the format in which it can be shared (printed, electronic, as a summary report, etc.) should also be described. ○ If there are concerns that Ministry of Health or other local officials will request identifiable data, this guidance will benefit from high level approval from the National AIDS Council or equivalent. • Type 2: sharing to support service delivery in a way that benefits the individual service user (e.g., when someone is referred between facilities) ○ Describe that identifying information can be shared **only with the informed consent of the client**. Mechanisms in place to share information, such as accompanied referral or written referral slips, should also be described. ○ Describe ways in which job responsibilities and geographic areas of work will dictate the identifiable information that is shared with individual IP staff or volunteers. For example, peer educators will need to have information that corresponds to the type of services they provide within the communities where they work. However, they should not have information about individuals in communities	Guidance for Type 1 data sharing (illustrative language): *When sharing information for data analysis and reporting, no identifying information (e.g., service user's name, email, address, phone number, date of birth) can be included. Information will not be disaggregated to such a level that it becomes possible to identify an individual. Information on location of individuals, including hot spots, should never be shared beyond the project. Data can be shared upon requests made to [insert staff person name and title] as summary printed and/or electronic reports.* Guidance for Type 2 data sharing (illustrative language): *Identifying information shared with service providers for the benefit of the service user (e.g., HIV status) requires the informed consent of the service user. This means the service user understands what will be shared, with whom, and why.* *Peer educators will have access only to identifiable information that they collect or that corresponds to relevant service history (such as condom distribution) in those geographic areas where they work. They should not have specific individual's clinical results (e.g., HIV and STI testing results) or anything else disclosed to other project staff in confidence (e.g., experiences of violence) unless the individual has given informed consent for this to be shared. They may have aggregate data on incidents of violence at a hot spot in their geographic area to understand HIV vulnerability.* Another example for Type 2*: When using an electronic client management system like ORA or QuickRes it will store client appointment and service access*

beyond their geographic purview and should not have access to clinical results (such as HIV or sexually transmitted infection [STI] test results), or other information that a service user shared with health care workers (HCWs) or other program staff (such as experiences of violence) unless the service user has consented that this information can be shared.	*data and share access to multiple systems users: clinic staff, case managers, outreach workers, and program managers and M&E staff. The consent form on ORA/QuickRes will explain what client data is shared with which users. Clients do not have the option to use ORA/QuickRes if they do not agree to these data sharing parameters. Separately, online outreach workers and others should be trained to ask for client consent when they use ORA or QuickRes on behalf of a client or when they reassign client records to other users on the system (such as reassigning the client's appointment to another clinic or case manager).*
14. Does the implementing partner keep a list of individual(s) with the right to destroy data if its protection cannot be guaranteed due to an emergency? • Provide the names and positions of those who can destroy identifying data outside of compliance with donor specifications in case of an emergency (a general rule of thumb is to keep paper data for five years; for organizations with clinical files, follow Ministry of Health rules and policies regarding data storage). Clearly outline when such a decision can be made and by whom and have it reviewed and approved by the donor(s) to your program.	Names and positions of staff with right to destroy data (illustrative language) *Destruction of data should be the last option and used only if there are no other alternatives to protect data. Data can be destroyed if it is not possible to protect identifiable data (the program data is under threat). The decision that such a threat is imminent can be made by [name and title].*
15. Is a protocol in place for the safe destruction of records? • Each donor will have their own guidelines regarding how long paper and electronic records must be kept. Follow these guidelines unless there is an emergency that requires earlier destruction of data (see #13). • Electronic data should be destroyed completely. Note that simply deleting a file does not destroy it. Choose from the destruction options described here: https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Best%20Practices%20for%20Data%20Destruction%20%282014-05-06%29%20%5BFinal%5D_0.pdf. • If needed, paper records should be destroyed using cross-cut shredders, pulverizers, or incinerators.	How long should paper data be stored? How long should electronic data be stored? Specific guidance from the Ministry of Health on the storage of clinical records How paper-based records will be destroyed How electronic records will be destroyed Documentation of past data destruction, including date and method used

• Destroy CDs, DVDs, and any magneto-optical disks by pulverizing, cross-cut shredding, or burning. • The process of how data will be destroyed, including on what timeline, should be included. This can serve as the protocol. • Each time data is destroyed the process for destruction should be described in detail and signed by the person who has destroyed the data. • Review the protocol quarterly to ensure that it meets your needs and reflects your current staffing structure.	
16. Does the implementing partner obtain informed client consent before their data is entered into program databases? • Consent form (paper or electronic) should explain the types of data that may be collected, who has access to view/use it, and the data protections in place. Generally, choosing not to give consent means data for the individual cannot be entered into the system. However, the user can consent to provide information and then simply withhold information they do not wish to share. • Program staff who enter client data on behalf of clients are trained to explain to clients the consent form/data use and privacy policy and obtain/document their consent before proceeding to enter their data.	Client consent forms Data use and privacy statement

Section 4. Staff Training and Management

Instructions	Documents to support operationalization (with illustrative examples)
17. Were all program staff trained in data confidentiality within the past year? • Training should include skills building on how to encrypt and password protect electronic files. • Training in confidentiality should cover ○ Who will be responsible for collecting and recording information ○ Where and how information will be collected and recorded ○ How information will be stored ○ Who will have access to the information, including what information will be shared within a facility or with third parties (such as providers within a referral network) ○ How to ask clients for informed consent before collecting their data • The training will also describe the consequences of sharing identifying information.	Training content developed List of trained staff with date of each person's training Client consent form/data use and privacy policy

18. Are protocols in place to guide action in case individuals intentionally violate data confidentiality regulations? • Intentionally violating data confidentiality regulations—for example, sharing a client file with another staff person who should not have access to it—will be grounds for employment termination. Large-scale breaches in confidentiality—such as sharing a database—or the use of client records for purposes such as blackmail will be prosecutable under local law as long as such action does not endanger the project or any of those it serves. • Accidental breaches in confidentiality require retraining and may result in reduced staff responsibility (including less or no access to records). • Violations of confidentiality should be documented, with outcomes recorded. • Verbal disclosure of confidential client information—such as a peer educator disclosing a client's HIV status in conversation—should also be documented and include appropriate consequences, such as retraining or termination, based on the severity and intentionality of the disclosure. This document focuses on breaches involving written or electronic data. For more on any breach of confidentiality, refer to the Oath of Confidentiality in the Program Monitoring Guide (p. 22), which should be signed by each implementing partner staff who has access to confidential information.	Record of breaches in confidentiality, including: date, person who committed breach, description of incident, outcome for the project, and disciplinary action taken against staff person Signed Oath of Confidentiality for each implementing partner staff; this document should be signed upon completion of confidentiality training and indicate that the worker: (1) completed the training, (2) understands how to maintain and protect personal information, (3) understands their responsibilities to report any observed violations, and (4) understands the consequences of violating client confidentiality