DATA.FI REPORT

Data Access and Security Standard Operating Procedure for Client Management Information System Data

Kingdom of Eswatini
Ministry of Health, Health Management Information Systems Unit

SEPTEMBER 2022

PEPFAR
U.S. President's Emergency Plan for AIDS Relief

USAID
FROM THE AMERICAN PEOPLE

Data.FI
Data for Implementation

September 2022

Suggested citation: Data.FI. (2022). Data Access and Security Standard Operating Procedure for Client Management Information System Data. Washington, DC, USA: Data.FI, Palladium

Table of Contents

FIGURES

Abbreviations

CMIS	Client Management Information System
DMT	Data Management Team
HMIS	Health Management Information System
KP	key population
MOH	Ministry of Health
PEPFAR	United States President's Emergency Plan for AIDS Relief
SOP	standard operating procedure
TBD	to be determined
USAID	United States Agency for International Development

Document ID	
Date of Issue	2022
Version	1.0

Revision History

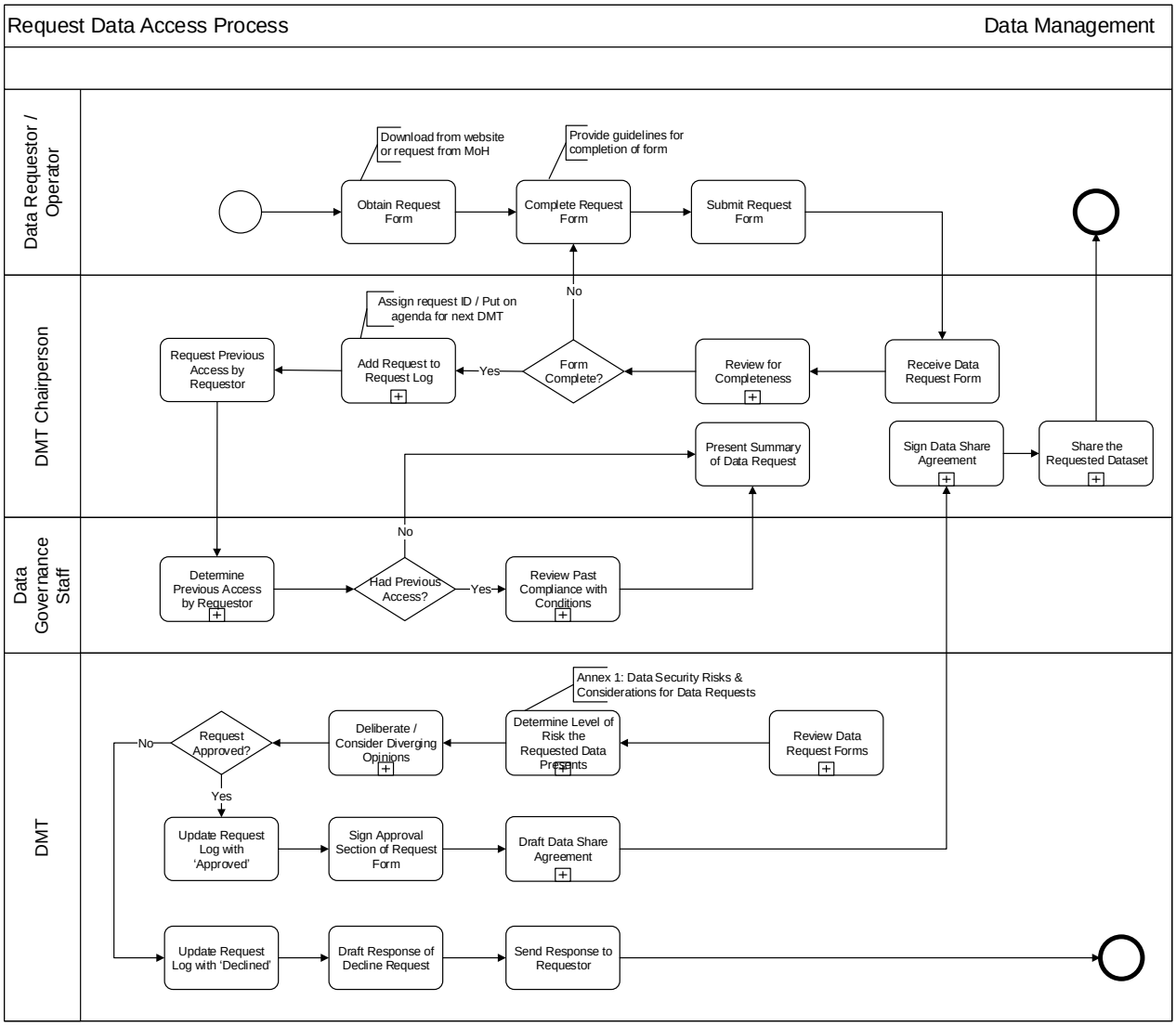
Date	Version	Description	Author

PURPOSE

This standard operating procedure (SOP) is to guide the Data Management Team (DMT) and the Chairperson to decide whether to grant data access to external parties, and to provide details on how to share the requested data. This SOP not only aims to increase efficiencies and standardize the process, but is also primarily concerned with ensuring security and privacy are considered in the decision-making process. There is an inherent tension between data security/privacy and data accessibility/usability that this SOP considers.

The SOP has two sections: the first is on **CMIS Data Access and Security,** which is primarily concerned with the process of receiving, reviewing, and granting data access requests. The second section, **Shared Data Governance**, instructs staff on the procedure that must be followed to ensure proper documenting and tracking of data that have been shared. This is especially important for overall data governance of the Client Management Information System (CMIS) to know what data sets have been shared but is also critical in cases where “live” data are shared with external groups. For example, if dynamic data are shared but it is later discovered that the data contained errors, corrective action would need to take place to update the data set, and to alert the data operator. Or, if personally identifiable information or other sensitive data were accidentally shared in a data set, documentation would allow the responsible team to quickly see what data sets needed to be retracted.

Figure 1. Data access process summary



Procedure for CMIS Data Access and Security	
Responsible	**DMT Chairperson**
Actors	DMT, data requestor/data operator, data governance staff
1.1	Data requestor visits Ministry of Health (MOH) website and downloads data request form (https://www.gov.sz/index.php/health-documents)
1.2	Data requestor gathers required materials and fills out and submits the form online.
1.3	Data request form received by the Chairperson, reviewed for completeness; if incomplete, sends it back to the requestor; if complete, logs the request, assigns a request ID, and puts it on the agenda for the next DMT meeting.
1.4	Chairperson sends a request to data governance staff to consult the shared data inventory to see whether the same organization or individual has previously gained access to the data.
1.5	If so, the data governance staff need to review past compliance with the conditions (i.e., sharing of publications produced through the use of MOH data).

1.6	At the DMT meeting, the Chairperson presents a summary of the request, including the applicant's prior access to data and compliance with conditions.
1.7	DMT reviews the data request forms and determines what level of risk the requested data present according to Annex 1. Data security risks and considerations for data requests.
1.8	The DMT considers whether the data should be shared, and if so, at what level of granularity based on the request, the use case, potential risks, and whether the applicant may have access to additional data that could help reidentify any deidentified data.
1.9	DMT deliberates and hears any diverging opinions.
1.10	Chairperson of the DMT makes the final decision.
1.11	If the data request is granted, the request log is updated to "approved" and the Chairperson completes the data request form with his/her signature and approval. Note: the request log should be kept secure and only accessible to members of DMT/data governance staff.
1.12	If the data request is not granted, brief reasons for the decision are shared with the data requestor and the request log is updated to "denied."
1.13	The DMT notifies the requestor, who is now referred to as the "data operator" and provides a timeline for when the requestor will receive access.
1.14	The DMT creates a data sharing agreement between the MOH and the data operator based on available data sharing agreement templates. The data sharing agreement stipulates the conditions from the data access request form, and additional conditions and requirements based on the specific data being shared. The agreement will provide the period of time that the data can be used, how the data will be shared, stored, when it should be destroyed by the data operator, and how to notify the HMIS in the event of a data breach.
1.15	The Chairperson will share the data sharing agreement with the data operator for review and signature. The data operator will then return the agreement to the Chairperson before data access is given.
1.16	The Chairperson compiles the requested data and creates or imports a metadata file with details about the data set. The metadata will later be referenced to ensure that no changes have been made since granting access.
1.17	The Chairperson shares the data set with the data requestor via a one-time online access code on an encrypted service (SharePoint link, Dropbox Link, Mimecast, etc.).

Procedure for Shared Data Governance	
Responsible	**TBD**
Actors	DMT, data requestor/data operator, data governance staff
2.1	To be determined (TBD) will review the Shared Data Inventory on a monthly basis and make any updates based on new data access, revoked access, etc., as required.
2.2	Reviews any dynamic data sets for end dates on their access.
2.3	Where required, revokes access manually or checks to see that the link to access will expire on the correct date.
2.4	Reviews any updates from partners on published work and creates a report to share with the MOH.
2.5	References assigned Data Request # and acts on any relevant considerations.
2.6	On a monthly basis, data governance staff review a random selection of 20% of shared data sets to ensure that the data set has remained consistent with metadata (I.e., deidentified data are still deidentified, key population (KP) is not distinguished in a non KP data set).

Annex 1. Data Security Risks and Considerations of Data Request

Request Type #	Data Request	Risk level (1-5 low to high)	Considerations
1	▪ Report with static[1] aggregated data not including KPs ▪ Report with dynamic, aggregated data not including KPs ▪ Deidentified static data set not including KPs ▪ Anonymized static data set not including KPs ▪ Any static data not related to health facility location or patient data ▪ Any dynamic data not related to health facility location or patient data	1-2	Monitor data set to ensure that no permissions/settings have changed.
2	▪ Report with static aggregated data specific to KPs ▪ Report with dynamic aggregated data specific to KPs	2	Consult data sharing policy for MOH decisions on the sensitivity of KPs. Monitor context for increased stigmatization of KPs. Monitor data set for any changes in disaggregation or granularity.
3	▪ Dashboard, map, or other similar platform with dynamic[2] aggregated data not including KPs	2	Monitor data set to ensure that no permissions have changed/drill down have been enabled.
4	▪ Dashboard, map, or other similar platform with dynamic aggregated data specific to KPs	2	Monitor data set to ensure that no permissions have changed/drill down have been enabled. Monitor context for increased stigmatization of KPs.
5	▪ Deidentified static data set specific to KPs ▪ Deidentified dynamic data set not including KPs ▪ Anonymized dynamic data set specific to KPs	4	Monitor data set to ensure that no permissions/settings have changed. Monitor context for increased stigmatization of KPs. Conduct review of data openly available to determine whether identification of deidentified data set is possible (Mosaic Effect[3]).
6	▪ Deidentified dynamic data set specific to KPs	5	Monitor data set to ensure that no permissions/settings have changed. Monitor context for

[1] Static data: A fixed data set, "a snapshot in time." Examples include a written report with qualitative and quantitative data, a visualization (map, chart, graph), or an Excel sheet.
[2] Dynamic data: A data set that evolves or is added to and will be updated. Access to a dynamic data set requires a live connection via an Application Programming Interface (API), an online dashboard, or other online tool.
[3] Mosaic Effect: When combinations of data sets from various sources allow the user to produce the "whole picture" that was not previously viewable in any single data set. This can lead to reidentification of deidentified data.

			increased stigmatization of KPs. Conduct a review of data openly available to determine whether identification of deidentified data set is possible (Mosaic Effect).
7	▪ Static data on health facility location ▪ Dynamic data on health facility location	TBD	Highly dependent on context. Are healthcare facilities for KPs being targeted? Consult MOH

Annex 2: Revised Data Request Form, 2022

DATA REQUEST FORM

The Ministry of Health of the Kingdom of Eswatini encourages all interested users to request data sets/ data through the Health Management Information Systems (HMIS) Unit. Users are required to submit a request for data, providing the HMIS Unit with information on the specific data requested and the intended use. Submission of the data request form does not guarantee access. Upon submission of the completed data request form, the HMIS Unit will review the request and decide whether to grant access, grant modified access, or reject the request.

Please complete the form below

Name of requestor:	
Organization/Institution:	
Address:	
Cellphone:	
Email address:	
Country:	
Data/data sets being requested. (Please be as explicit as possible by including data variables, indicators of interest, etc.).	
Reason for request (motivation and intended use. Please provide details on whether, where, and how outputs of the data will be shared/published).	
Data Access: who, if anyone, besides yourself will have access to the data? For what purpose?	
Data parameters: Start date	
Data parameters: End date	
Please elaborate on the specifics of the data being requested: (national, regional, local) and disaggregation required (sex, age, KP status, etc.)	
Are you aware of any data that the MOH has previously shared with you? If so, please list the data sets and the data request access ID number associated with the data set.	
Estimated date of project/research completion for which the data are being requested.	

What is your preferred format for the data? Please note we will do everything within reason to provide you with your preferred format, but it is not guaranteed. Select all that apply:	☐Report (PDF, MS Word) ☐ .CSV ☐ Map ☐ Graph/Chart ☐ HTML ☐ Dashboard
Date of submission:	

Please read the following agreement. All users of all the data sets agree to the conditions listed below. Submission of the completed data request form and signature below qualifies as acceptance of the following conditions and is required.

Conditions

1. The user agrees that the Ministry of Health, through the Health Management Information Systems (HMIS) Unit is the owner of the data set(s).
2. The user agrees that the data set will be used only for the purpose requested and will not share the data set with others.
3. The use of these data sets in research communication, scholarly papers, journals, and routine data use for reporting is encouraged, but the authors of these communications and documents are required to acknowledge/cite the Health Management Information System Unit as the source of the data.
4. All scholars, nongovernment partners and non-Ministry of Health requests for data are required to produce a letter from their institutions specifying why the data are requested.
5. A copy of all outputs (report, visualization, link, etc.) produced from the data set for the reasons of publication or other forms of circulation should be submitted to the Data Management Chairperson of the DMT within 30 days of publication. Any user who fails to do so will be ineligible for future data access.
6. The user agrees that any use of the data or reliance by the user on any of the data is at the user's own responsibility and that the Ministry of Health shall not be liable for any loss or damage whatsoever arising as a result of such use.
7. The user agrees that he/she will not attempt to link or permit others to attempt to link the records of persons in these data sets with personally identifiable records from any other source.
8. The user agrees that he/she will make no statement or permit others to make statements indicating or suggesting that interpretations drawn are those of the Ministry of Health.
9. The user agrees that all information provided in the data request form is true and representative of the intended use of the data.
10. **PENALTY CLAUSE:** The user agrees that non-adherence to the above statements may result in the Ministry of Health not making available any data sets to the user in future.

Data Requestor full name	

Signature	
Date	

For Internal Use Only:	
Data Request Access ID Number:	
Data Request Type (1-7) (Annex 1. Data security & Considerations of Data request)	
Status (Approved/Declined):	
If the request is declined, state the reason(s):	
Date of approval/decline:	
DMT Chairperson:	
Date of data sharing	

Annex 3. Shared Data Inventory

Data Access Request ID	Data Request number (1-7) (Annex 1 Data Security Risks & Considerations of Data Request)	Date of sharing	Date sharing ends	Format of data shared (.CSV, PDF etc.)	Are the data static or dynamic? (i.e., does the user have access to data over time?)	Indicators shared	Received publication from data operator? (Yes/No)	Link to publication (If relevant)	Query/script used to develop data request

TL-22-47

Data for Implementation (Data.FI) is a five-year cooperative agreement funded by PEPFAR through USAID under Agreement No. 7200AA19CA0004, beginning April 15, 2019. It is implemented by Palladium, in partnership with JSI Research & Training Institute, Johns Hopkins University Department of Epidemiology, Right to Care, Cooper/Smith, DT Global, Jembi Health Systems, and Macro-Eyes, and supported by expert local resource partners.

SEPTEMBER 2022

FOR MORE INFORMATION

Contact Data.FI:

Brian Bingham, Data.FI AOR
bbingham@usaid.gov

Jenifer Chapman, Data.FI Project Director
datafiproject@thepalladiumgroup.com

https://datafi.thepalladiumgroup.com/

PEPFAR
U.S. President's Emergency Plan for AIDS Relief

USAID
FROM THE AMERICAN PEOPLE

Data.FI
Data for Implementation