Data.FI SOLUTIONS BRIEF

Protecting Health Records

DATA GOVERNANCE AND INFORMATION SECURITY

Medical records track clients across clinical services, improving continuity of care and the client care experience. Accurate and comprehensive health records, either in physical or digital form, are essential for generating high-quality data for clinical performance monitoring and case-based surveillance, informing client-centered approaches, and enabling cohort analyses and program monitoring. If mishandled or used for unauthorized purposes, health records can also present risks for clients, namely unintended harm or social stigma. Data governance policies and information security controls must be in place to mitigate the risks and maximize monitoring, surveillance, and service-delivery benefits.

THE OPPORTUNITY

Although the availability of timely, accurate, client-line information at scale can accelerate epidemic control, in countries supported by the United States President's Emergency Plan for AIDS Relief (PEPFAR), electronic medical records (EMRs) are implemented at varying levels of resource and scale. Adapting and refining information security controls according to local conditions is therefore vital. Implementing partners must be prepared to address the particular risks associated with operating in low-resource environments as well as in countries with mature, well-resourced EMR implementations.

Moreover, data governance—local regulations, clearly defined information flows, stakeholder roles, and responsibilities—is critical for defining both information security controls and the appropriate access for stakeholders to longitudinal records and de-identified data sets. Information security controls must be aligned to existing information flows and defined stakeholder roles to ensure that data access is based on a need-to-know basis and only to the appropriate level of disaggregation.

If constructed purposefully, data governance and information security guidelines can mitigate risks to participants and ensure that data are collected through managed processes that ensure quality, accountability, systems integration, and that support decision making.

THE DATA.FI SOLUTION

Our approach to information security optimization involves assessing the local context, identifying gaps, and catalyzing local leadership to design and implement standard operating procedures (SOPs) that guide routine operations to deliver improved accountability and data governance. We work in tandem with local partners to then implement SOPs—ensuring country ownership, developing local capacity, and facilitating the implementation of supporting management structures.

Step 1: Design SOPs to fit local governance context

Data.FI identifies and engages with local authorities and relevant stakeholders to assess the tools and structures in place to collect, manage, share, utilize, and dispose of health records. Depending on the local context, we may apply any or all of the following three components:

- **Governance:** Assess the enabling environment, including policies, operational guidelines, management structures, information flows, roles, and responsibilities.
- **Infrastructure:** Assess available non-digital infrastructure including service sites, record storage facilities, and paper record management protocols. Also, assess available digital infrastructure including workstation management, information systems security, and business continuity procedures.
- **Gap analysis:** Assess how routine practices differed from established data management guidelines (if available). Ensure data management guidelines include secure practices for handling physical and digital records.

The assessment is completed over a two-week period through a combination of key informant interviews, user observation, system demonstrations, detailed software reviews, and reviews of available records. Following the assessment, Data.FI drafts information security SOPs and leads the review with health authorities and technical teams to validate the document and plan its implementation.

Step 2: Implementation of SOPs

The SOPs outline practices, roles, and responsibilities to strengthen information security through participants' health record lifecycle. The SOPs may include guidelines and controls for:

- Sharing participants' records during activity implementation
- Storing physical and digital records
- Protecting devices that access participants' records
- Reporting and responding to a data breach
- Establishing non-disclosure agreements for staff and volunteers accessing participants' data

If the country has EMR systems in place, the SOPs may also include:

- Procedures to ensure the EMR solution is up to date with the latest security patches
- Procedures for securing local area networks and preparing workstations accessing the system
- Documentation of stakeholders, system roles, and access rights
- Procedures, roles, and responsibilities to manage user accounts
- Procedures, roles, and responsibilities to ensure business continuity

If local authorities are required to share their data, the SOPs may also include:

- Data-sharing agreement to engage with donors and partners working in-country
- Authorship agreement to engage with external entities developing knowledge products

WHAT IS THE IMPACT?

Data.FI has developed and is working to implement new information security SOPs in several countries, ensuring new guidelines and tools respond to the local context and that local capacity is developed to implement and improve secure practices over time.

In **Zimbabwe**, Data.FI led a cross-partner community of practice to define new information security guidelines and delivered workshops to strengthen governance and use of data across implementing partners working on HIV programming using a DHIS2 platform. We also supported the review and improvement of existing information security guidelines in **Burundi**, where data is collected using and EMR solution at 300 sites, and in **Eswatini** we are developing local capacity to manage their EMR system currently in use at more than 200 sites.

We are also improving information security in countries where an EMR system is not yet available. In **Guatemala** we are working at the district level and supporting the implementation of best practices to increase information security at service sites to reduce risks to participants and collaborators.

PUTTING THE SOLUTION INTO ACTION

Data.FI works with country programs to identify opportunities to strengthen their information management practices with increased security. We collaboratively develop context-aware procedures, including best practices and guidelines based on the country's objectives, operating environment, and the maturity level of the health information system. Data.FI can develop and support implementation of the SOPs through the following:

- Assessing EMR solutions and addressing information security gaps
- Facilitating alignment among stakeholders and coordinating security management
- Assessing and addressing information governance gaps and security risks
- Developing local capacity to implement and manage information security

SB-23-01

Data for Implementation (Data.FI) is a five-year cooperative agreement funded by the U.S. President's Emergency Plan for AIDS Relief through the U.S. Agency for International Development under Agreement No. 7200AA19CA0004, beginning April 15, 2019. It is implemented by Palladium, in partnership with JSI Research & Training Institute (JSI), Johns Hopkins University (JHU) Department of Epidemiology, Right to Care (RTC), Cooper/Smith, DT Global, Jembi Health Systems, and Pendulum, and supported by expert local resource partners.

July 2023

FOR MORE INFORMATION

Contact Data.FI

Madeline Schneider, Data.FI AOR
mschneider@usaid.gov

Shreshth Mawandia,
Data.FI Project Director
datafiproject@thepalladiumgroup.com

https://datafi.thepalladiumgroup.com/