Global Digital Health Network
Formerly the mHealth Working Group

PEPFAR

USAID
FROM THE AMERICAN PEOPLE

Palladium
MAKE IT POSSIBLE

Data.FI
Data for Implementation

GDHN October 2023 Webinar

Information Security for International Development Projects: How do we protect personal identifiable information (PII) when digital solutions are not available?

Early Bird registration for the Global Digital Health Forum ends October 13. Register now.

Global Digital Health Network

TechChange

Global Digital Health Forum 2023

December 4- 6, 2023

Hybrid Event - Virtual (Asia and East Africa time zones)

In-Person - Washington D.C.

Starting October 14, in-person D.C. ticket rates will increase to $998.

Global Digital Health Network

User-centered Information Security

In international development programming

October 12, 2023

Nonye Nwanya and Eric Ramirez

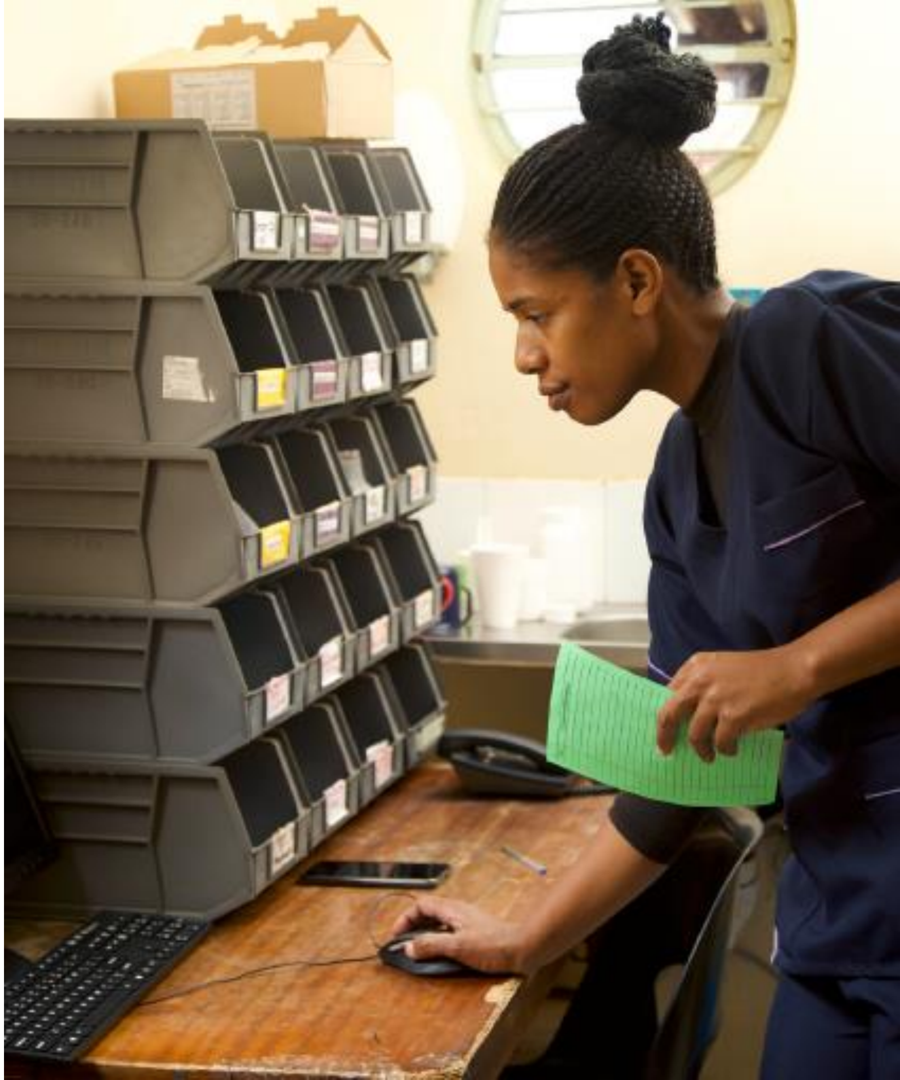
PEPFAR

USAID FROM THE AMERICAN PEOPLE

Data.FI Data for Implementation

Agenda

- Introduction to Information Security
- Information Security Controls and Certifications
- In-country Approaches
- Sample Approach Application
- Data.FI experience



Information Security

An Introduction

What is Information Security?

Protect information and **information systems** from unauthorized access, use, disclosure, disruption, modification, or destruction
in order to provide integrity, confidentiality, and availability.

Source: National Institute of Institute of Standards and Technology (NIST)

What’s included in an information system?

What’s Included in an Information System?

A	B	OPTIONS
• Web Pages • Tablets and Phones • Servers • User Computers • Everything IT	• Office Space • Paper Records • People • Program Guidelines • Everything Non-IT	1. Only A 2. A and pieces of B 3. Everything from A and B

What is the Context?

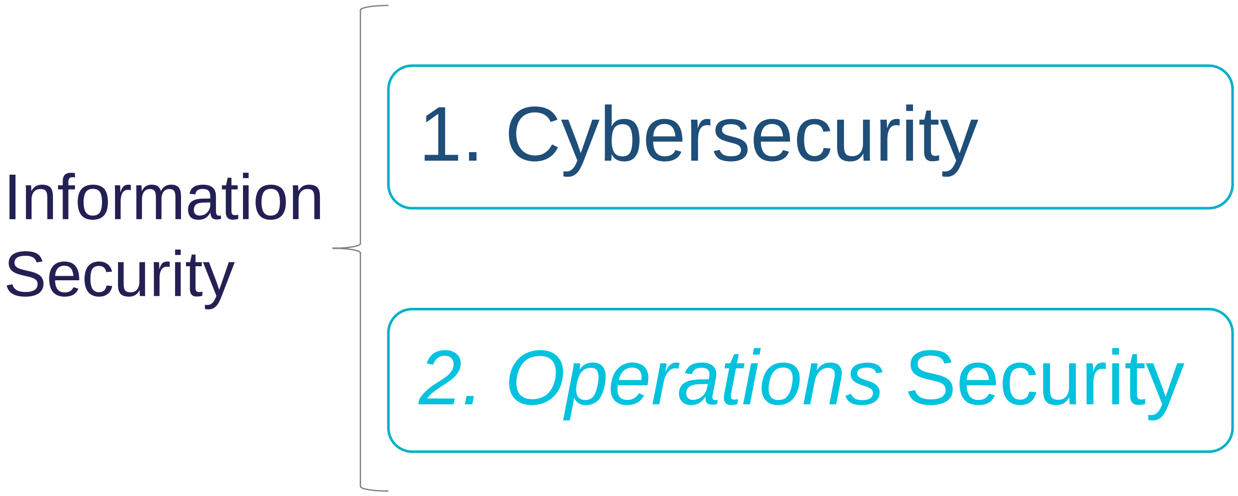
Security must cover available information in both digital and non-digital formats.

Context: Low- and middle-income countries (LMICs) where digital uptake is lower.

Demand: Participants' records contain sensitive information, especially in health programming.

Scope: We must protect the entire information system – not just tech; most projects still use paper records as part of their routine operation.

Components of Information Security



Information Security

1. Cybersecurity

2. *Operations* Security

RISK MITIGATION

Digital hygiene, secure software development and deployment, etc.

Process guidelines, protection of physical assets, etc.

Do projects include an information security policy? YES/NO

And Do they include both areas of risk mitigation? YES/NO

Protecting the Entire System

An information system (IS) is an organizational solution designed to collect, process, store, and distribute information. It is composed of tasks, people, roles, and technology.

Source: Wikipedia

Controls need to be established to manage these components.

Whose job is it? (Operations)

e.g., Should a data entry clerk ask for an ID? Should a MEL officer access personal information? How long should information be retained?

Information Security

Controls and Certification

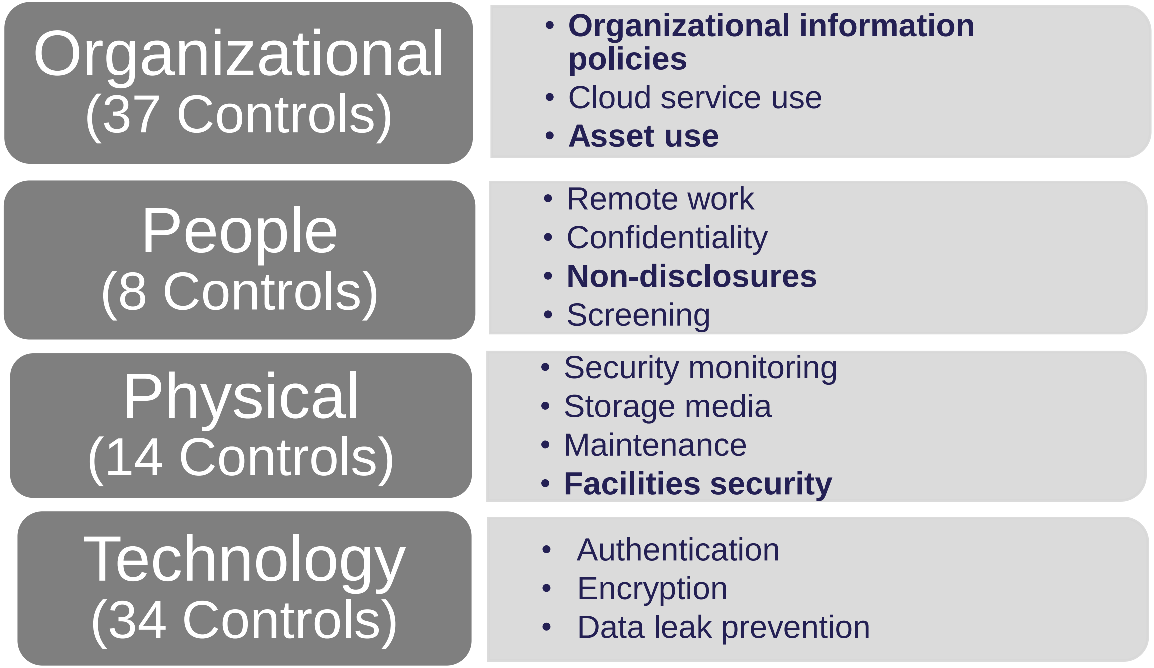
About Security Certifications

- Information security certifications provide a recognized set of controls that attest to an organization’s security standing.
- Organizations can implement information security controls and have an independent audit to certify their compliance.
- Security certifications are also industry driven; organizations obtain them to gain a competitive advantage.

ISO 27001 Certification

International Standards Organization’s (ISO) Information Security Management System certification **includes 93 controls** under four domains. Palladium obtained this certification last year (version 2013)

*version 2022



Organizational
(37 Controls)

- **Organizational information policies**
- Cloud service use
- **Asset use**

People
(8 Controls)

- Remote work
- Confidentiality
- **Non-disclosures**
- Screening

Physical
(14 Controls)

- Security monitoring
- Storage media
- Maintenance
- **Facilities security**

Technology
(34 Controls)

- Authentication
- Encryption
- Data leak prevention

USAID Security Policies

USAID manages mandatory policies (Automated Directive System - ADS) to meet requirements from the Federal Information Security Modernization Act of 2014 (FISMA).

- **ADS 545** Information Systems Security: Information security for the information and information systems that support the operations and assets of the Agency, including those managed by contractors on USAID's behalf.
- **ADS 552** Cyber Security for National Security Information (NSI) Systems: Applies to USAID classified data, national security information systems.
- **ADS 540** Development Experience Clearinghouse: Covers information products from USAID's programs such as text, images, video, audio, maps, charts.
- **ADS 579** Development Data Library: Covers structured datasets, raw data created or obtained with USAID funding.

Information Security

Palladium's Approach

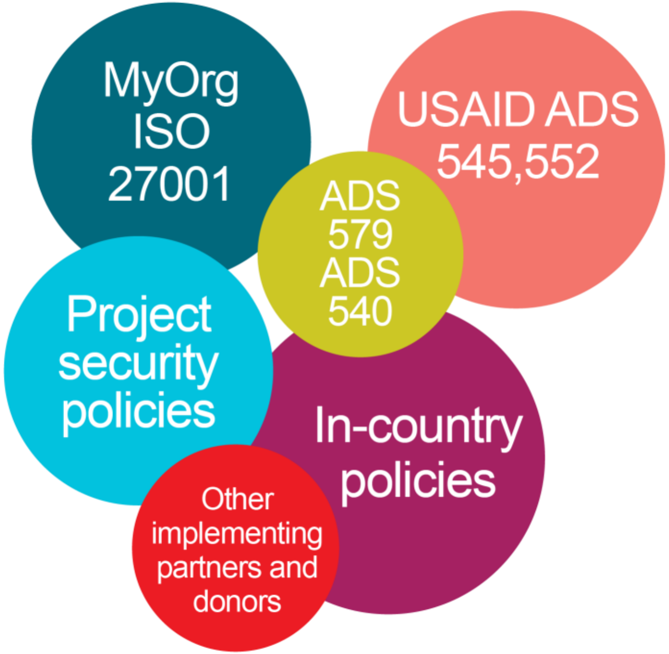
In-country Project: Which Approach?

Existing security controls/certifications are implemented within the organization.

In-country projects need to respond to the local capacity, laws, and context.

Given the limitation in resources, what should be our approach?

Consider: tasks, roles, people, and technology



Information Security in the Local Context (1)

An approach to designing security policies in development programming

- 1/4 Tasks: Understand programmatic needs and expected outcomes, develop workflows and identify key tasks. Identify and document risks (e.g., What data do we need? Are we visiting participants?).

- 2/4 Roles: Define responsibilities, controls, and checks. Ensure roles, controls and checks are enforced either manually or through technology (e.g., Who needs access data? How long do we need to keep data?).

Information Security in the Local Context (2)

An approach to designing security policies in development programming

- 3/4 Technology: Identify what can be automated and what needs to be completed manually. Prefer well tested/documented/supported solutions that follow best practices (i.e., enforced passwords, 2FA, etc.)

- 4/4 People: Manage change; explain program goals, end-to-end information flows, risks and controls/checks, and the need for compliance. Train in the completion of manual procedures and the use of technology.

What Does This Look Like in Practice?

Example: We have been hired to improve linkage to care for HIV patients at the community level in 'SpringField,' a country with 10 million inhabitants and a nominal GDP of $5k per-capita. Our client wants us to show evidence of information security protocols and guidance to protect client data.

- What are the tasks needed to complete our project?
- Which people/skillsets do we need in our team?
- What roles would people play, and how do we train them?
- Do we need to collect data? If so, how (paper forms, web forms)?
- Which types of data do we need (DOB, Address), and why?
- Are there local data protection regulations we should incorporate?

A Very Simplified Summary (based on our example)

Task	People/Role	Technology /Tool	Control
Register and triage patients	Nurse/ Data entry	Paper forms	Signs a non-disclosure agreement that includes data protection regulations (refer to any National Data protection Acts, donor regulations e.g., USAID 545). Nurse accounts for and securely stores paper forms and tablets at the end of the workday. Nurse confirms/signs facility log, reports incidents.
Track progress at community-level	M&E Officer/ data collation	Excel	M&E Officer ensures Excel files are password protected and shared using secure methods (corporate online drive) – no public file sharing services. Use only official email accounts to share access to files.
Assess progress, review campaign priorities	Immunization director/s	Excel	Director organizes/mandates/verifies trainings for team members; investigates/documents reported incidents; verifies compliance with national and donor policies.

Data.FI’s Experience

Data.FI Brings Together Leaders Across the Digital Health and Analytics Landscape to Harness the Power of Data to Save Lives

We scale global goods and local solutions for efficient and equitable health programming and epidemic control

WHO WE ARE

Data.FI is a global health field-support mechanism implemented by:

- Palladium (prime)
- JSI Research and Training Institute
- Right to Care
- Pendulum
- DT Global
- Johns Hopkins University
- Cooper/Smith
- Jembi Health Systems

Data.FI is supported by a community of resources partners including Fraym, IBM, Premise, Regenstrief, and others.

The project accepts **PEPFAR, COVID-19 and health** funding and has a $180M ceiling.

WHAT WE DO

Digital health system enhancement and scale-up, and data system integration to transform health care

Data analytics that enable precision programming and resource optimization

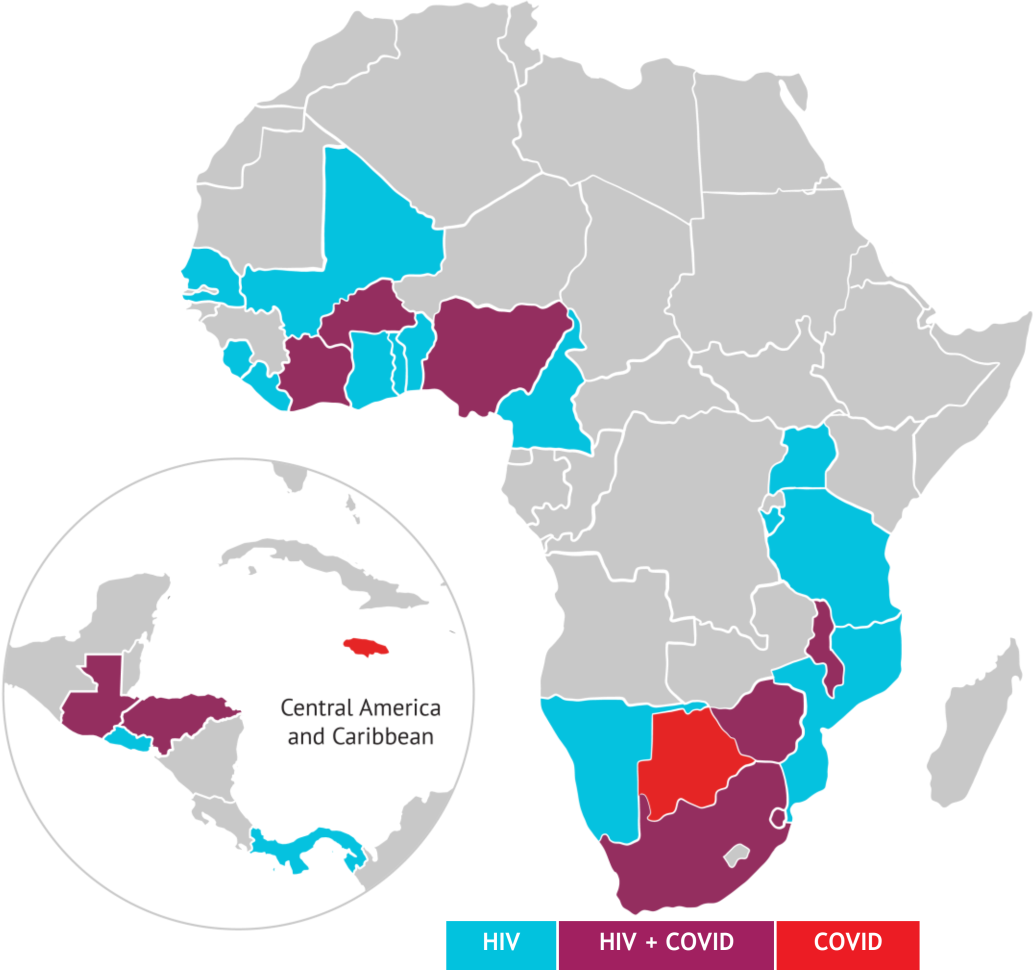
Decision-support interventions to optimize health care performance and efficiency at all levels

Local governance structures that set standards, enable system integration and data access, and ensure data quality and security

We enable local stakeholders to drive sustainable, country-led solutions, strengthening local data ecosystems

Learn more: https://datafi.thepalladiumgroup.com/

Data.FI is working with local stakeholders to optimize country health information systems and health system performance in more than 20 countries



*Data.FI also has health funding in Tanzania and Guatemala

Data.FI's Approach to Information Security in Field Programming

- Engage with stakeholders – implementing partners, donors, and local authorities
- Understand context (digital maturity, local regulations, etc.)
- Define scope (people, process, data)
- Assess risks (operational, digital, non-digital, etc.)
- Design controls and guidelines
- Sensitize and train users

Data.FI’s Approach to Information Security in Low-resource Environments

We work alongside other implementing partners and local health authorities to assess the local context and develop **Information Security Guidelines/SOPs**, which specify:

- Applicable local data protection regulations
- How records are shared with implementing partners during activity implementation
- How physical and digital records are stored
- Processes for identifying, reporting and responding to an incident
- Requirements for non-disclosure agreements for staff and volunteers accessing sensitive and private data
- Authorship agreements with external entities who are supporting the development of knowledge products.

The SOP document is built collaboratively with, and owned by, the local health authorities.

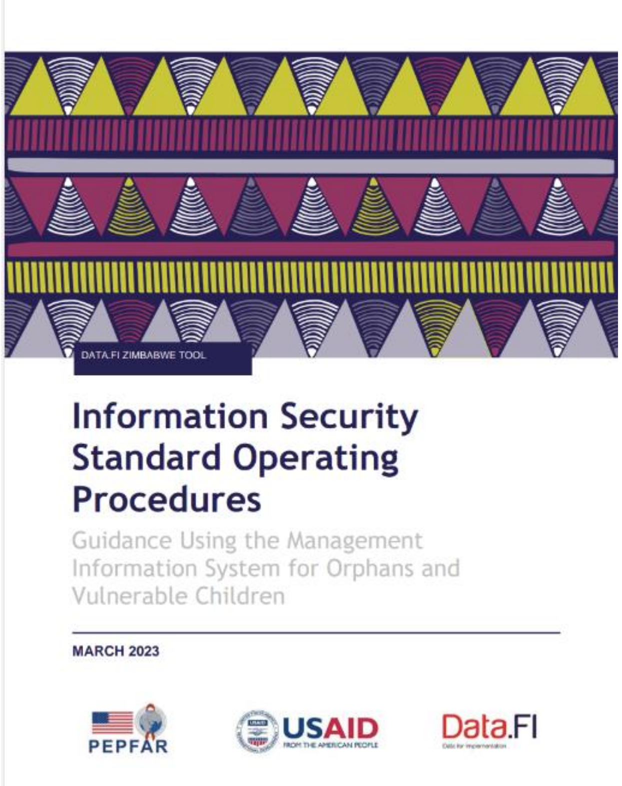
Data.FI's Approach to Information Security of Digital Systems

We also work in countries that have **digital solutions at the health facility level** and develop guidelines that may include**:**

- Procedures for securing local area networks at the health facilities
- Procedures for securing workstations accessing the system from health facilities
- Documentation of user groups, system roles, and access rights
- Procedures, roles, and responsibilities to manage user accounts
- Procedures, roles, and responsibilities for data backup and restore procedures
- Procedures to ensure that electronic medical record (EMR) components are up to date with the latest security patches

The SOP document is built collaboratively with, and owned by, the local health authorities.

Example



DATA.FI ZIMBABWE TOOL

Information Security Standard Operating Procedures

Guidance Using the Management Information System for Orphans and Vulnerable Children

MARCH 2023

PEPFAR

USAID
FROM THE AMERICAN PEOPLE

Data.FI

- Multiple implementing partners
- System accessed at facilities across the country
- Services implemented at the community level

Challenges

Challenges encountered in operationalizing information security processes include**:**

- Less control in enforcing the information security SOP
- Implementing partners provide oversight to the facility level users
- Different organizational policies on implementation processes across implementing partners
- User creation and management is done at the implementing partner level
- User access management to the web version of the EMR is done by the implementing partners

In Closing …

1. Most of us are thinking about cybersecurity, which is good, but not enough. Information Security is not exclusive to digital solutions, especially in international development projects, and there is no one-size-fits-all solution.
2. Beyond an information security certification, our community needs to think about security in the local context of the local environments, projects, and partners.
3. Identifying project risks associated with people, processes, and data allows us to assign accountability and design appropriate controls.

Thank you!

Please share your questions and comments

FOR MORE INFORMATION

Madeline Schneider, Data.FI AOR, USAID Office of HIV/AIDS
mschneider@usaid.gov

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

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.

This presentation was produced for review by the U.S. President’s Emergency Plan for AIDS Relief through the United States Agency for International Development. It was prepared by Data for Implementation. The information provided in this presentation is not official U.S. government information and does not necessarily reflect the views or positions of the U.S. President’s Emergency Plan for AIDS Relief, U.S. Agency for International Development or the United States Government.

PPT-23-75

Join the next GDHN webinar

Digital transformation lessons learned from the USAID funded Country Health Information Systems and Data Use Project (CHISU) and the Ethiopia Digital Health Activity (DHA)

When: November 15 @ 9:00 EST (New York/UTC-5)

Hosted by: JSI

More details and registration link coming soon!

Global Digital Health Network
Formerly the mHealth Working Group

Join the GDHN!

Global Digital Health Network
Formerly the mHealth Working Group

https://bit.ly/GDHNSignUp