Neglected tropical diseases (NTDs) are a diverse set of 20 diseases and disease groups with a singular commodity: their devastating and disproportionate impact on impoverished communities. Untreated, NTDs can lead to life-altering disabilities that prevent patients from working, attending school, and gaining socioeconomic mobility to name a few. Great strides have been made to eliminate or control the spread of preventative chemotherapy diseases such as onchocerciasis, trachoma, schistosomiasis, soil-transmitted helminths, and lymphatic filariasis through donor- and community-led mass drug administration (MDA) campaigns and government action. As countries move towards national goals and targets, the need for reliable data management and secure data systems are required for the preparation of elimination dossiers, drug applications, and to inform preventative chemotherapy diseases such as onchocerciasis, trachoma, donor- and community-led mass drug administration (MDA) campaigns and management. While governments across West and Central Africa are adopting national data strategies, Ministries of Health (MOH) often do not have formal data security policies in place to secure the protected health information of their patients. For national NTD Programs (NTDPs), data are often stored on unsecure Excel sheets or on personal devices of health staff. NTDPs have acknowledged the need to standardize how their data are stored to ensure data integrity, analysis, and validation of their data, and protect data from possible inaccuracies and loss. Supporting NTDPs across eleven West and Central African countries, USAID’s Act to End NTDs | West supports the NTDPs in evaluating data security policies using leading global references such as the U.S. National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity and USAID’s Digital Strategy for 2020-2024. The NIST Framework provides the basis for Act | West’s four-phase approach developed to support NTDPs to improve data security policies, illustrated below in Figure 2. At the forefront of this approach are facilitating collaboration and encouraging ownership of this process by relevant stakeholders from all levels of the health system such as community drug distributors, regional health data managers, and NTDP directors. This is reflected from the initial stages of research and analysis of data security current practices to the national level workshop in Phase 3.

Examples of concrete data security procedures to adopt include fully integrating NTD data entry and storage into existing national health information platforms; establishing clear roles and responsibilities for the protection of physical and digital data; and investigation of lost/missed data; installing firewalls and antivirus software and acquiring centralized storage servers; improving and expanding data management trainings to more data management staff; clearer guidelines on securing data storage; and identifying various software to invest in and adapt for NTDP data collection purposes, e.g., District Health Information System 2, Epi Info, SPSS Statistics, Open Data Kit (ODK), PowerBI, Evernote, and RedCap. In drafting these policies, participants consider the level of effort, resources (e.g., human, financial), and stakeholders required for effective implementation. This process also allows NTDPs to map out, in detail, the flow of data from the point of data collection during community MDA campaigns to reporting to influence national-level decision-making. By the end of the methodology, stakeholders have identified and drafted NTDP data security policies, illustrated below in Figure 2. At the forefront of this approach are facilitating collaboration and encouraging ownership of this process by relevant stakeholders from all levels of the health system such as community drug distributors, regional health data managers, and NTDP directors. This is reflected from the initial stages of research and analysis of data security current practices to the national level workshop in Phase 3.

As more countries push for increased digitalization and data-driven solutions, the creation, documentation, and implementation of data security policies are essential. This work helps to guarantee that programmatic and health system data are secure and reliable, supporting sustainable health programming.

REFERENCES


ACKNOWLEDGEMENTS

This poster presentation is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the sole responsibility of the Act to End NTDs | West program, led by Philanthropies in partnership with Helen Keller International and Health Development International, Deloitte, World Vision, and the American Leprosy Missions under Cooperative Agreement No. 7200A-19CA00011 and do not necessarily reflect the views of USAID or the United States Government.