

CASE STUDY ON 'PROTECTING PERSONAL HEALTH INFORMATION FOR PLHIV AND KEY POPULATIONS'

Context

In many countries, people living with HIV (PLHIV) are likely to encounter stigmatisation and discrimination. This can range from loss of employment and housing to actual bodily harm or even death. This is accentuated by the fact that, in many countries, the incidence and prevalence of PLHIV is higher in communities that are already marginalised. These include men-who-have-sex-with men, sex workers, people that use drugs and other key or vulnerable populations. As countries develop HIV prevention and treatment cascades and use national health identifiers (NHIDs) to track PLHIVs and other key populations within national health services or programmes in the era of Big Data, the issue of protecting personal health information has become an acute and pressing problem.

Introduction

In 2007, UNAIDS and PEPFAR (President's Emergency Plan for AIDS relief) developed guidance for countries to allow them to protect the confidentiality and security of personal health information of PLHIV¹. This formed the basis for country guidelines to ensure the confidentiality and security of all personal health information, which were developed and published in 2016². These guidelines also developed and field-tested tools to use in clinics, data warehouses/repositories and at national level that allow countries to assess the confidentiality and security of personal health information.

Aims

To field test the paper-based and electronic tools for assessing whether personal health information that has been collected, stored and used is adequately protecting the confidentiality and security of this information at clinic, data warehouses /repositories at national level verify the existence and implementation of national guidelines.

Method

A paper-based assessment tool was developed and field tested in Jamaica in 2014 and is now accessible via the UNAIDS Website³. This formed the basis for developing an electronic version of the Tool, using an ODK (Open Data Kit) platform for Android devices. The smartphone version was field tested in Jamaica in August 2018.

Results

The field test for the paper-based version found it an effective and efficient method of assessing whether the personal health information at clinic, data warehouse/repository national levels was adequately protected and for verifying the existence and implementation of national guidelines. The electronic version, using smartphone technology on the ODK platform, was even more efficient than the paper-based equivalent and very user friendly.

Recommendations

All countries need to develop guidelines to protect the confidentiality and security of personal health information. They also need to assess, on a regular basis, the extent to which these guidelines are being implemented at clinic, data warehouse/repository and national levels, using either the paper- or electronic based tools. Based on the outcome of these assessments, countries can then make the relevant improvements required.

References:

- 1) http://data.unaids.org/pub/manual/2007/confidentiality_security_interim_guidelines_15may2007_en.pdf
- 2) <https://www.tandfonline.com/doi/full/10.3402/gha.v9.32089>
- 3) http://www.unaids.org/en/resources/documents/2016/confidentiality_security_assessment_tool

Authors: Eduard J Beck*, Wayne Gill**, Paul De Lay***

Organisation: NPMS-HHC CIC*; Ballsille School of International Affairs**; Global Health Consultant***

Date: 11-11-2018

Email: ejbeckphase2017@gmail.com; gillw77@gmail.com; pkdelay11@me.com

Phone Number: + 1 514 586 7584