DHIS 2 Android App Implementation Guidelines

Table of Contents

Executive Summary

Background

The University of Oslo in response to the growing smartphone adoption rates in Sub-Saharan Africa and developing countries, added to the clear leadership of the Android Market Share, decided to build a new Mobile DHIS 2 Android Application, DHIS 2 Capture Android, which was released in September 2018. This work builds upon the lessons learnt from the previous mobile DHIS 2 Android Apps: Data Capture, Tracker Capture, Event Capture and Dashboard.

The DHIS 2 Capture Android Application is designed to facilitate working in settings with poor or no connectivity, since it allows the user to work offline and synchronize the data later when connectivity is available. It makes data collection easier, by bringing all DHIS 2 data models into a single, consolidated app. It is envisioned to be used by health workers (front line workers, service providers, health centers staff…) at health facilities and work directly done at community level.

DHIS 2 Capture Android Application is different from the web-based DHIS 2. The web-based DHIS 2 is meant to be used where users have access to larger screens and good internet connection. The Android App has been designed taking into consideration the user experience with smaller screens and with poor or no connectivity.

Research shows that a mobile eHealth App can be easily integrated into care, improving productivity. The App should facilitate client follow-up, data reporting, and decision-making. However, the feasibility and usability of the app can be negatively affected by high beneficiary volumes, staff shortages, and problems with the software and the devices. Real time monitoring, program investment and the right human resources will be needed for a successful integration of mobile client data apps for frontline health workers in rural and resource-poor settings (Rothstein JD1 et al. 2014).

Objectives

The objective of this document is to provide a set of guidelines for the deployment of the Mobile DHIS 2 Capture Android Application. The steps of the deployment, which will be described in detail later in the document, include:

1. Security and Data Protection aspects
2. Mobile devices requirements
3. Installation and Setup
4. Testing (internal testing and user acceptance test)
5. Field testing and Piloting
6. Scale up (app distribution, mobile device management, training)
7. Rollout.

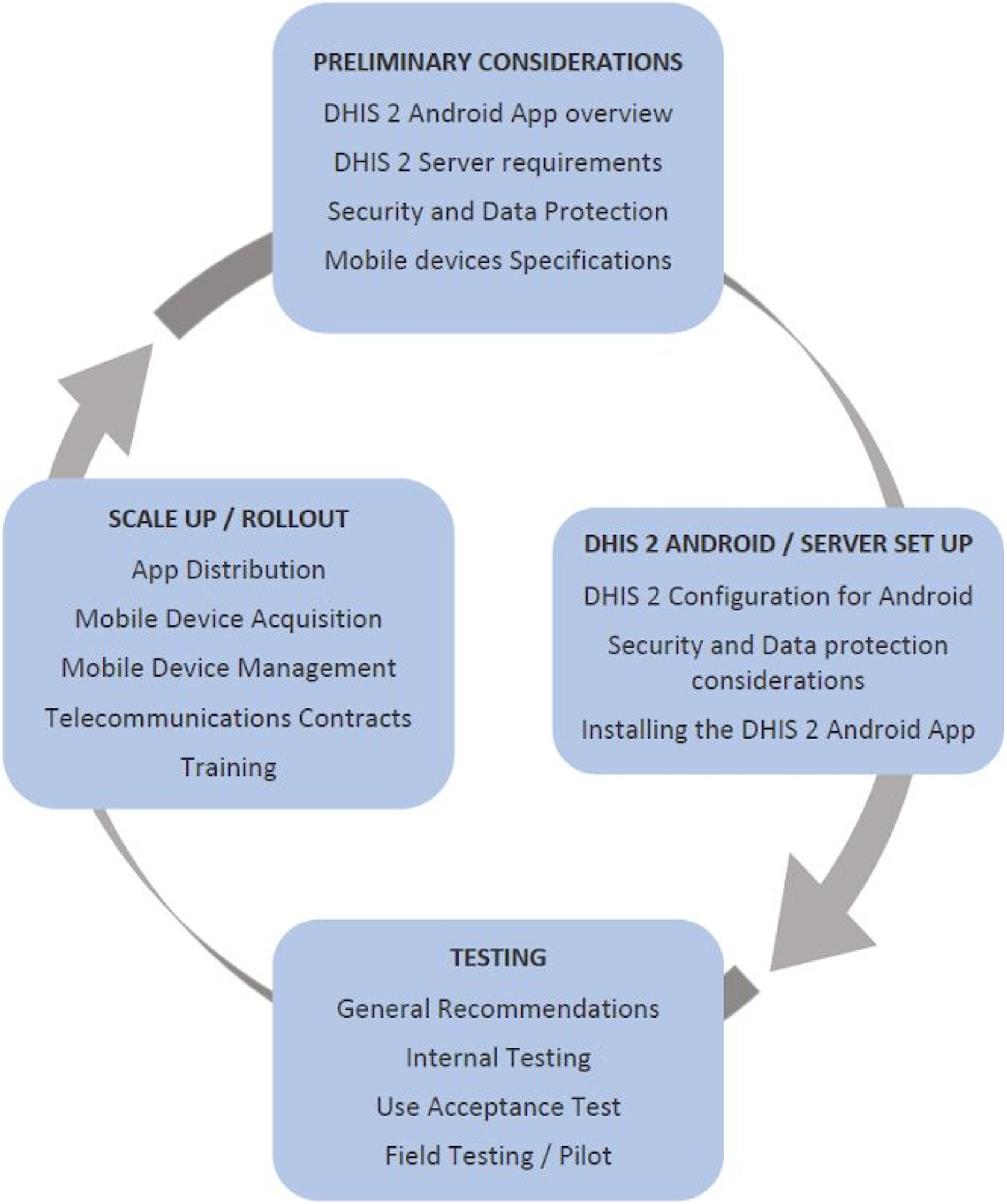
It is also included a document map which groups the sections of the document into the phases of a mobile implementation project. All aspects here represented should be considered at the beginning of the project and planned accordingly. This representation illustrates in which phase of the project they will be of critical importance.which summarized its key aspects and facilitates following up this guidelines in your project. It is important to highlight that the *cycle represented in the document map* considers the requirement gathering process finished. The document map can be found in the first section.

In the last section, it is included a checklist which summarized its key aspects and facilitates following up this guidelines in your project.

Target Audience

This document is intended to be used by those leading the deployment process from its early phases, and should be shared with those involved in the process.

Document Map



PRELIMINARY CONSIDERATIONS

DHIS 2 Android App overview

DHIS 2 Server requirements

Security and Data Protection

Mobile devices Specifications

DHIS 2 ANDROID / SERVER SET UP

DHIS 2 Configuration for Android

Security and Data protection considerations

Installing the DHIS 2 Android App

TESTING

General Recommendations

Internal Testing

Use Acceptance Test

Field Testing / Pilot

SCALE UP / ROLLOUT

App Distribution

Mobile Device Acquisition

Mobile Device Management

Telecommunications Contracts

Training

DHIS 2 Capture Android overview

This document focuses on mobile implementation which use the new DHIS 2 Capture Android App. To get additional information about the different DHIS 2 Android apps please visit the App store and the Documentation on the website. The previous set of DHIS 2 Android Apps developed are currently (2019) under corrective maintenance support only.

The new DHIS 2 Capture Android App allows offline data capture across all DHIS 2 data models*. Data and metadata are automatically synchronized whenever there is internet access, always keeping the most relevant data for the logged user in the local device.

Easier Login and enhanced data protection

Server URL can be set via a QR code. The app will also remember previous used URLs and user names. Once a user is logged, a four digit PIN can be used to secure the app with a soft log out.

Configurable App theme and Icon

The appearance of the app, including icon and color is determined by your server configuration. You can create a shortcut to the app with your institutional logo in the home screen of the mobile device by using the App Widget.

Attractive, user friendly navigation

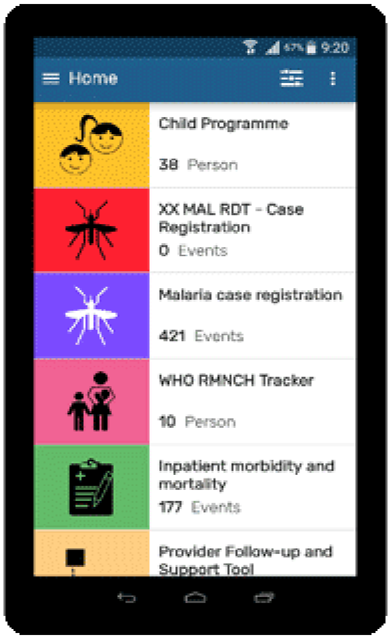
All programs and datasets* accessible to the logged user are integrated into the new "Home" screen.. Each program or dataset will be, displayed with their associated icon and colour.

Fully functional while offline: intelligent sync.

A local database in the mobile device keeps a synchronized copy of the DHIS 2 programs and datasets available to the logged user. The most relevant data is also automatically synchronized.

- Tracked Entities: by default, up to 500 active enrolments, prioritizing the most recently updated on the user's assigned data capture Org Unit(s).
- Events & Datasets: by default, the most recent 1,000 events or 500 datasets.

These parameters are configurable



Child Programme
38 Person

XX MAL RDT - Case Registration
0 Events

Malaria case registration
421 Events

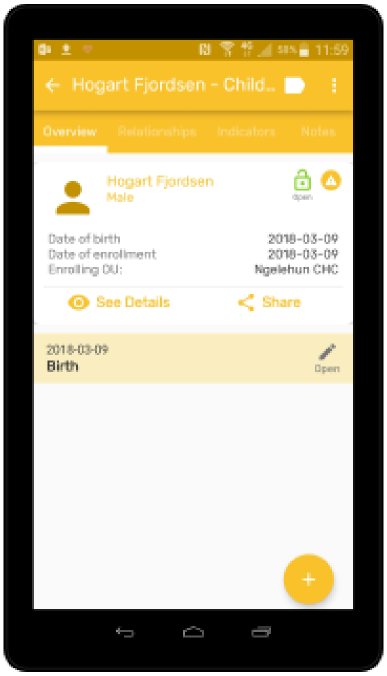
WHO RMNCH Tracker
10 Person

Inpatient morbidity and mortality
177 Events

Provider Follow-up and Support Tool

Tracker dashboard

DHIS 2's powerful tracker data model has been fully implemented in the small screen. The tracker dashboard incorporates feedback, relationships, indicators and notes. The app implements tracker logic by supporting most program rules, giving the possibility to add, schedule or refer new events, depending on the server configuration.



Hogart Fjordsen
Male

Date of birth 2018-03-09
Date of enrollment 2018-03-09
Enrolling OU: Ngelehun CHC

2018-03-09
Birth

Integrated search for tracker

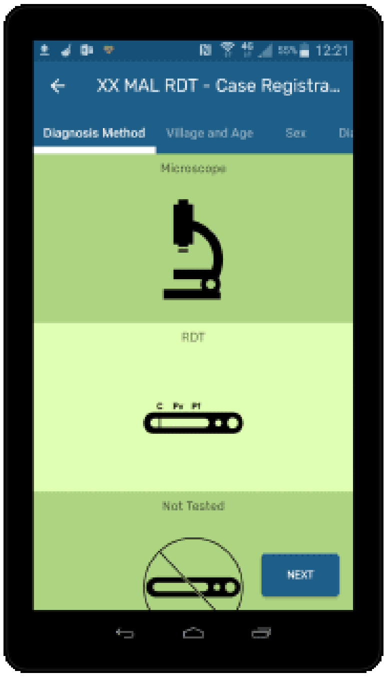
Before being able to add a new tracked entity, the app automatically conduct a search. If offline, the search is on the local synchronized database. and when online, it will suggest records for download, based on user's Organization Unit search configuration. This functionality minimized potential duplicates, even when the user is offline.

Pictorial Data Entry

Data Entry comes to life - icons and colors can be used to illustrate questions' answers. Available for data elements with associated options sets in both, single event and tracker programs.

Event Completeness

During data entry, the app will display information about the current status of completion for a program stage. Useful for complex surveys with multiple sections.



DHIS 2 Server Requirements

The new DHIS 2 Capture Android App requires a DHIS 2 2.29 or greater instance running in a web server. The DHIS 2 instance can reside on on-premise server, a virtual machine or it can be purchased as software-as-a-service (managed hosting). For more information about the different DHIS 2 hosting options please visit https://www.DHIS2.org/hosting.

This section provides basic guidelines on how to configure the DHIS 2 server, which you will need to do in the first two scenarios (on-premise and virtual machine). In the third scenario of managed hosting, you should let your provider know that you will be deploying the Android App and have an open discussion on best ways to configure the server. You could start by sharing these guidelines with your managed hosting provider.

The DHIS 2 Server must be designed and configured keeping in mind: data collection flow, expected data analysis and expected visual UI. At a minimum three servers will be needed for a DHIS 2 deployment: Testing, Production and Training.

The Testing Server will be the server where you can change the server configurations and test the results of such configurations. Once you are happy with the configuration, training of users should occur in an environment different to Production. A dedicated Training Server is the ideal environment in which you will train your users. You will create DHIS 2 users for all the trainees and make sure everyone understands and feels comfortable with the changes. The last step once you have tested the configurations and trained the users will be to deploy the configuration to the Production environment. You should never make configuration changes or train your users directly into the Production environment.

DHIS 2 is licensed under BSD, an open source license and is free for everyone to install and use. However, managing a DHIS 2 instance involves more than setting up a powerful web server. Deploying a reliable and scalable system includes at least these aspects:

- ❏ Human resources with skills in relevant technologies such as web servers and database systems.
- ❏ Reliable backup of your system including safe storage at a remote server.
- ❏ Use of SSL (HTTPS / encryption) to keep private information like passwords secure.
- ❏ Monitoring of server resources and application performance.
- ❏ Stable and high-speed Internet connectivity.
- ❏ Stable power supply including a backup power solution.
- ❏ Secure server environment to avoid unauthorized access, theft and fire.
- ❏ Powerful hardware with potential for scaling together with increased system usage.

The DHIS 2 Capture Android App runs in mobile devices, including smartphones, tablets and chromebooks. It is important to keep an eye on the number of programs, number of data elements and number of program rules that are made available to a user on those mobile devices. You should also budget sufficient time for creating the necessary translations for your metadata configuration. For the app dialogues, menus and other prompts, if the app is not translated to the language that you need, please send us a message in the DHIS 2 community and we will let you know how to contribute to the app translations.

Data Security and Privacy

With the new DHIS 2 Android Capture App, users will be collecting individual data at the point of service provision, which is the lowest level of direct data capture as it involves the direct beneficiary. Capturing Data this way enables upstream analytics without compromising on detail, makes downstream analytics possible, reduces error and enables post hoc analysis to answer questions identified after data collection and system design. However, individual data brings additional challenges for information systems, including considerations of security and privacy, considerations of readiness and capacity, as lower IT literacy data collectors are provided with digital tools and additional complications with regards to analytics, storage and system responsiveness.

There is wide consensus on the need to provide a comprehensive data security practice. This comprehensive security practice should consider not only *confidentiality* and *integrity,* but also *availability of data*. Harvard Humanitarian Initiative has stated that information itself, including its generation, communication and reception, is a basic humanitarian need that should be afforded protection equal to other such traditional needs as food, water, shelter, and medical care. The Roadmap for Health Measurement and Accountability (MA4Health), stated that "Public health and clinical care cannot be delivered safely, with high quality, and in a cost-effective manner, without seamless, sustainable and secure data and information exchanges at all levels of the health system". Still, the capture and storage of personally identifiable data introduces risk and a commensurate obligation for rigorous privacy practices.

The University of Oslo is committed to the following:

1. Ensuring that the DHIS 2 software development and release process is subject to a transparent and rigorous security verification plan;
2. Through an action research approach, the university seeks to learn by doing in solidarity with others;
3. Striving to develop, learn and share relevant, timely and useful information and tools to promote good security practice;
4. Access to any and all health information in the course of our practice will be governed by strict and mutual agreement;
5. Using the university's actions to provide good example of security practice.

There can be a tension between the health system's need for identifiable data, and the patient's right to privacy. In the absence of clear legislation governing the collection and storage of personally identifiable data, there are important concepts that should be understood and promoted by system owners and implementers. They include:

❏ **Right of access**. The right of access will be defined by the data protection regulations of each country. In general terms, it includes information about the processing purposes, the categories of personal data processed, the recipients or categories of recipients, duration of storage, information about the rights of the data subject such as rectification, erasure or restriction of processing, the right to object, information about the existence of an automated decision-taking process, including profiling, etc. Please be aware of the regulations specific to your area and make sure you are ready to comply before you start collecting data.

❏ **Right of erasure**. The right of erasure is also defined by the data protection regulations of each country. In general terms, personal data must be erased immediately where the data are no longer needed for their original processing purpose, or if the data subject has withdrawn his/her consent and there is no other legal ground for processing. Again please make sure you understand the regulations of your specific area and make sure you are ready to comply.

❏ **Data minimization**. The basic idea of data minimization is that data processing should only use as much data as is required to accomplish a given task. It also implies that data collected for one purpose cannot be used for another purpose other than original processing one without further consent.

❏ **Pseudonymization**. It is a data management procedure that makes personal data less identifiable while keeping it suitable for analysis and processing. It can be accomplished by replacing the value of some of the data fields by one or more artificial identifiers, or pseudonyms. Pseudonymized data can be restored to make individuals identifiable again, while anonymized data can never be restored to its original state. Depending on the regulations applicable to your area, you can define a Pseudonymization strategy that meets the regulations and meets your needs.

❏ **Traceability**. In order to use data effectively we need to ensure its integrity. In order to ensure its integrity, it is important to monitor these data when they are collected, processed and moved. You need to understand: "what", "when", "why" and "who". Organizations that take advantage of traceability, are able to find data faster and are better able to support security and privacy requirements.

Based on the regulations of your territory and the complexity of your project, including the level of potential risk, you must implement appropriate technical and organisational measures, such as pseudonymisation, data minimisation, audit logs, search restrictions, granular sharing, etc, and integrate the necessary safeguards into the data processing in order to meet the requirements of the regulations that apply to your region.

An adequate security / privacy approach for any DHIS2 implementation capturing personally identifiable data would include the creation of a clear policy naming an individual(s) with full access to the system, with the responsibility to ensure the following. For any technical support on databases containing sensitive data, a signed NDA with a clear end-date should be required for any third parties.

	Possible practical implementation
Right of access & Right of erasure	Giving access to the patient to his / her record electronically for its review or deletion is not available in DHIS 2 (2.32). You should ensure that you put in place other methods by which a patient can request a copy of his/ her record so he/ she can review it and request amendments or its deletion. If its deletion is not possible, you should anonymize the record by removing / replacing all identifiable data points.
Data minimization	Ensure that there is a valid reason for collecting personal identifiable data. Don't collect unnecessary details which don't serve a practical purpose in terms of data analysis or the need of finability of a patient record. For example, if the need for patient follow-up gets determined by a test result being positive, don't collect patient name if the result is negative.
Pseudonymization	Consider using alternative values for recording information about certain procedures or conditions of a patient. Por example you can have a list of medical procedures / personal behavior / actions listed as a color list. This allows to do analytics, without revealing what could be a stigmatized procedure/ action/ behavior in a given territory.
Traceability	DHIS 2 provides detailed audit log for each data point. This includes the tracing of data captured via its web tools (from 2.22), as well as imported or via Android (from version 2.27). Currently (2.32) DHIS 2 does not provide a full deletion / anonymization export option, as deletion of a value preserves previous data in the audit log. For this reason, any sharing of exported data to outside parties should include manual removal of sensitive / identifiable data.

For practical recommendations on configuring DHIS 2 to guarantee data protection and security, please read the Security and Data Protection Considerations section.

Mobile Device Specifications

If your project plans to do a large acquisition of devices, it is good practice to delay the bulk of the acquisition as much as possible. The idea is to get the best device that you can afford. Technology, and particularly mobile devices, evolves very rapidly. A given model is normally refreshed on an annual cycle, giving consumers access to significant technical improvements year-on-year, but with similar price point. More recommendations on acquisitions can be found in the Scale Up section.

Specifications for mobile devices to use the new DHIS 2 Capture Android App deployment are included in the following table (for the most up to date version of this recommendations please visit this link).

	Mobile phones	**Tablets**	**Chromebooks**
Construction	Probably the most important feature: this device is going to be doing a lot of field work, and it needs to last 2+ years		
Brand	If you are going to be responsible for managing a lot of devices, it is easier to stick to one brand		
OS	Minimum Supported: Android 4.4 (not recommended) Minimum Recommended for new devices: **Android 7.X** Recommended for new devices: **Android 8.X** or superior		Chrome OS devices are updatable to the latest version of Chrome OS for at least 5 years after release. Check here
Processor	Recommended: 4 cores, 1.2GHz		various
RAM	Minimum: 1Gb Recommended: 2Gb or more	Minimum: 1.5Gb Recommended: 3Gb or more	Minimum: 4Gb Recommended: 4-8Gb

Storage	Minimum: 8Gb Recommended: 32Gb DHIS 2 app do not uses much space. However, storage of personal images & videos uses a lot of space		Minimum: 16Gb. Recommended: 32-128Gb
Screen Size	Minimum: 4" Recommended: from 5.5”	Minimum: 7"	11” - 14”
	Mobile phones	**Tablets**	**Chromebooks**
Camera	Minimum: 5Mpx, with flash Recommended: at least 8Mpx, flash		optional
Accessories Case, Keyboard, External power	Consider an appropriate external cover and a screen protector. For tablets, consider an external keyboard for desk operation. Consider supplying an external power bank (10,000 mAh - 20,000 mAh)		USB 3G/4G modem Mouse WebCam
Connectivity	4G (LTE)/ 3G radio, **unlocked**. If importing devices, check the compatibility of frequency bands with local mobile operators. Bluetooth 4.0 or better. WiFi 2.4 GHz & 5 GHz.		Bluetooth 4.0 or better. WiFi 2.4 GHz & 5 GHz. External USB 3G/4G dongle or Wifi hotspot

DHIS2 configuration for using the Android App

This chapter includes the basic configuration aspects for a successful experience using the Android App to help understanding the implications of using the mobile component of DHIS 2. For a complete and successful implementation, please read the detailed and updated documentation to get all the information about configuring the DHIS 2 Server for using with the DHIS 2 Android Capture App.

Aspects of the setup of the new DHIS 2 Capture Android App included in this document are:

❑ Security related considerations

- ❏ Creating an Android user
- ❏ Visual Configuration
- ❏ Setting up the Program Rules
- ❏ Defining Program Indicators and Legends
- ❏ Reserved IDs

Security related considerations

Using DHIS 2 sharing and share restrictions

In this section we will share some tips on how to use DHIS 2 sharing and share restrictions to ensure that only the right users have access to records with identifiable information.

Here is a practical example of granular sharing and search restrictions in the context of a Health Care Center for Maternal and Newborn Care:

Midwife User Role

- ❏ Can search across three programs across all org units in the district
- ❏ Can enroll new pregnant women into ANC program
- ❏ Can add/edit events to clinical assessment program stage
- ❏ Can view all ANC data in own org unit

Lab tech User Role

- ❏ Can search across one program org units in the district
- ❏ Can add/edit events to lab program stage
- ❏ Cannot view clinical assessment stage

MOH Supervisor User Role

- ❏ Can view dashboard only

It is very important to have standard operating procedures (SOPs) as part of your Data Protection Strategy.

A SOP is a set of step-by-step instructions compiled by your organization to help you carry out complex routine operations such as those related to data security.

SOPs helps your organization achieving efficiency, quality and consistency, while complying with Data Protection regulations.

When defining your Data Protection SOPs you should address questions such as:

- ❏ What is the relevant existing legislation?
- ❏ Who is the named controller? Processor? Data Protection Officer?
- ❏ Who is tasked with reviewing audit logs?
- ❏ What is your process for removing old users?
- ❏ Bring your own device?
- ❏ Hardware security?
- ❏ Mutual Confidentiality Agreements

We include here some SOP Best Practices taken from the DHIS 2 Community Health Information System Guidelines document published by the University of Oslo:

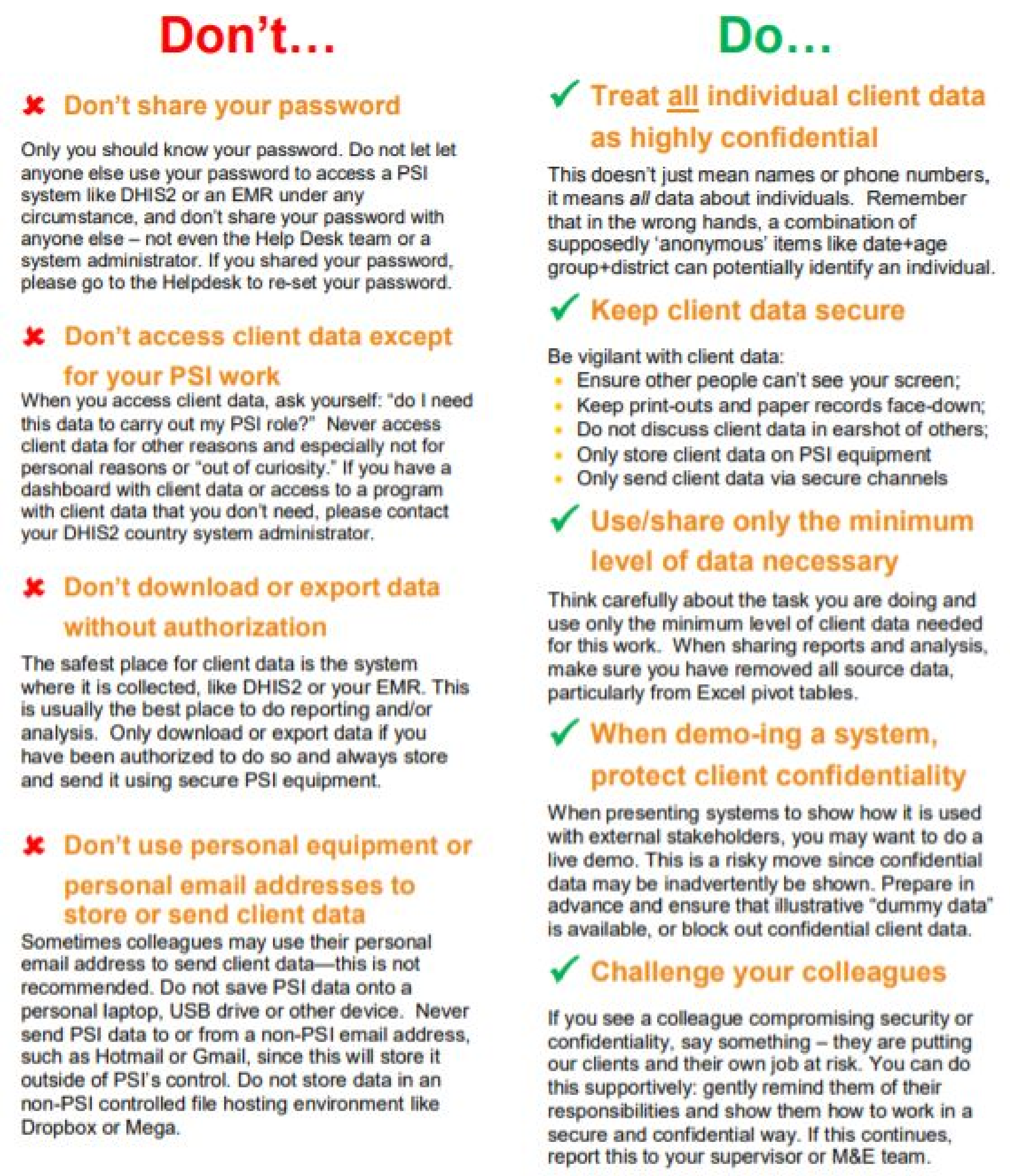
1. Harmonize multiple programs into a single data capture protocol.
2. Develop SOPs for each individual community project especially if multiple data flows exist.
3. Turn the SOP into illustrated posters and have the facility staff post them on their walls for public viewing.
4. Print SOPs and make sure all CHWs, facility staff, and district staff have copies
5. Stakeholders to sign the SOPs at the completion of training.
6. Stakeholder participation in the creation and approval of SOPs. The SOPs must institutionalize the best practices and workflow of the actors in the CHIS. Include representation from all relevant stakeholders in the process of developing SOPs.
7. Ensure all data elements and indicators are captured. The CHWs should clearly understand the meaning, and measurement of each data element and indicator to remove ambiguity
8. Use data capture guidelines at trainings. To build accountability, CHWs and facility staff need to know they are part of a larger system. They need to know how their data is used for planning at higher levels and specific actions at

lower levels.

9. Have the CHWs explain the data capture guidelines. This teach-back method is an effective adult learning practice. By explaining the data capture guidelines, this elevates the CHW's credibility with the health committee.
10. Produce, simple-to-use, local language guidelines. CHWs and facility staff need guides and instructions on what to do. Consider making posters or small laminated portable data capture guidelines for CHWs and facilities to put on the wall or carry with them that outline their role and responsibilities based upon the data capture guidelines.
11. Have CHWs, facility, district staff and national staff sign guidelines. This is a symbolic "commitment" measure. The aim is that they have read it, understand their reporting responsibilities as defined in the data capture guidelines, and will carry out these responsibilities.
12. Produce simple videos or audio and upload them to phones. Responsibilities and actions for every event are made easier with a simple, local-language videos or audio guides that facility staff and CHWs can refer to.

Practical Data Security Guidelines

Ensuring that the personal data stored on mobile devices is only accessible by the authorized health staff starts by educating users on how to use this data and ensure that it is kept secured at all times. The guidelines below are an extract taken from the PSI's "Monitoring and Evaluation Standard Operating Procedures for Keeping Client Data Secure & Confidential" manual.



Don't…

✖ **Don't share your password**

Only you should know your password. Do not let let anyone else use your password to access a PSI system like DHIS2 or an EMR under any circumstance, and don't share your password with anyone else – not even the Help Desk team or a system administrator. If you shared your password, please go to the Helpdesk to re-set your password.

✖ **Don't access client data except for your PSI work**

When you access client data, ask yourself: "do I need this data to carry out my PSI role?" Never access client data for other reasons and especially not for personal reasons or "out of curiosity." If you have a dashboard with client data or access to a program with client data that you don't need, please contact your DHIS2 country system administrator.

✖ **Don't download or export data without authorization**

The safest place for client data is the system where it is collected, like DHIS2 or your EMR. This is usually the best place to do reporting and/or analysis. Only download or export data if you have been authorized to do so and always store and send it using secure PSI equipment.

✖ **Don't use personal equipment or personal email addresses to store or send client data**

Sometimes colleagues may use their personal email address to send client data—this is not recommended. Do not save PSI data onto a personal laptop, USB drive or other device. Never send PSI data to or from a non-PSI email address, such as Hotmail or Gmail, since this will store it outside of PSI's control. Do not store data in an non-PSI controlled file hosting environment like Dropbox or Mega.

Do…

✓ **Treat all individual client data as highly confidential**

This doesn't just mean names or phone numbers, it means *all* data about individuals. Remember that in the wrong hands, a combination of supposedly 'anonymous' items like date+age group+district can potentially identify an individual.

✓ **Keep client data secure**

Be vigilant with client data:
- Ensure other people can't see your screen;
- Keep print-outs and paper records face-down;
- Do not discuss client data in earshot of others;
- Only store client data on PSI equipment
- Only send client data via secure channels

✓ **Use/share only the minimum level of data necessary**

Think carefully about the task you are doing and use only the minimum level of client data needed for this work. When sharing reports and analysis, make sure you have removed all source data, particularly from Excel pivot tables.

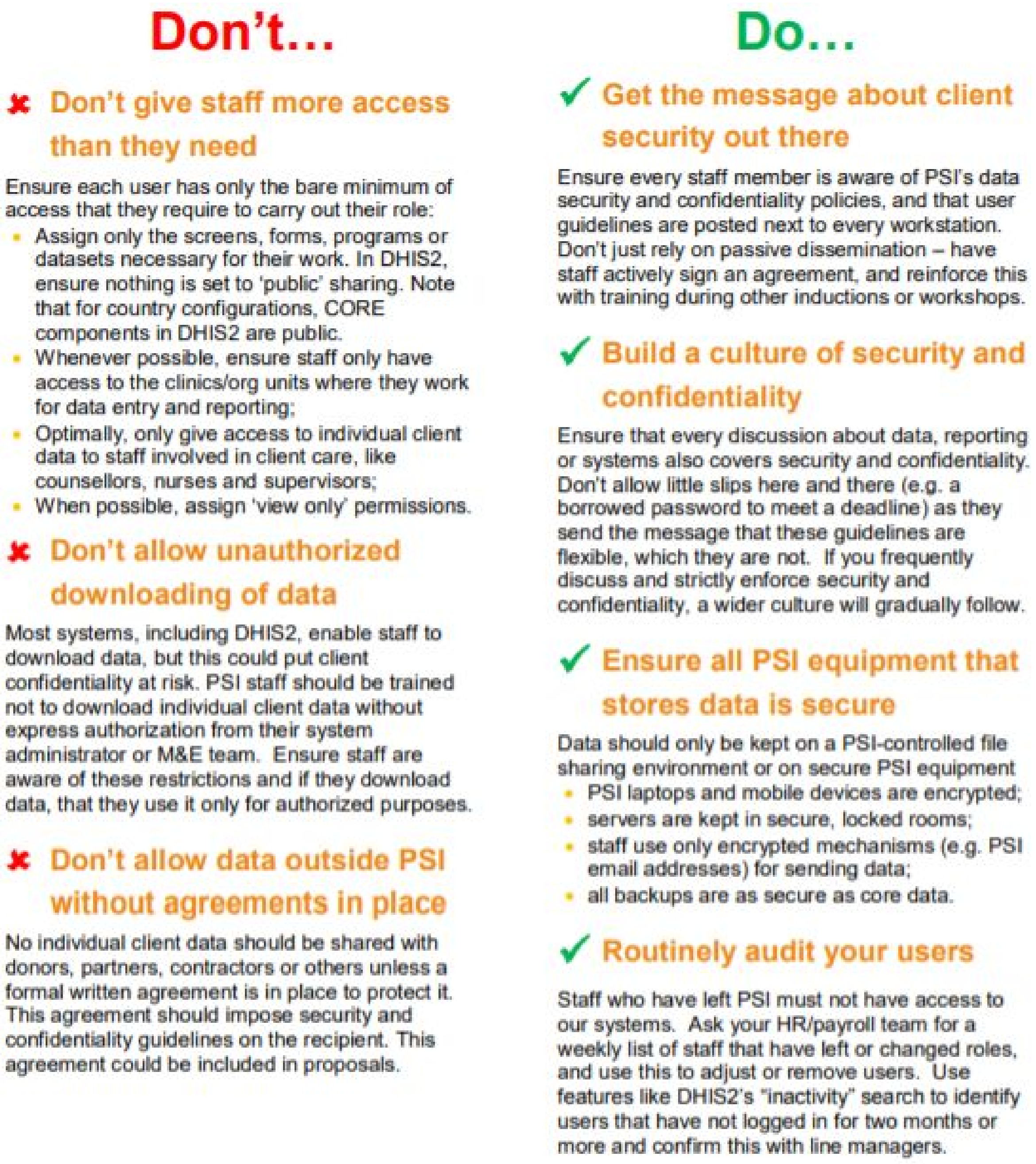
✓ **When demo-ing a system, protect client confidentiality**

When presenting systems to show how it is used with external stakeholders, you may want to do a live demo. This is a risky move since confidential data may be inadvertently be shown. Prepare in advance and ensure that illustrative "dummy data" is available, or block out confidential client data.

✓ **Challenge your colleagues**

If you see a colleague compromising security or confidentiality, say something – they are putting our clients and their own job at risk. You can do this supportively: gently remind them of their responsibilities and show them how to work in a secure and confidential way. If this continues, report this to your supervisor or M&E team.

System administrators play an important role when configuring user's access-level, by ensuring that their data access is appropriate and never unnecessarily execive. The guidelines below are also part of PSI's "Keeping Client Data Secure & Confidential Administrators Guide" manual.



Don't…

✘ Don't give staff more access than they need

Ensure each user has only the bare minimum of access that they require to carry out their role:

- Assign only the screens, forms, programs or datasets necessary for their work. In DHIS2, ensure nothing is set to 'public' sharing. Note that for country configurations, CORE components in DHIS2 are public.
- Whenever possible, ensure staff only have access to the clinics/org units where they work for data entry and reporting;
- Optimally, only give access to individual client data to staff involved in client care, like counsellors, nurses and supervisors;
- When possible, assign 'view only' permissions.

✘ Don't allow unauthorized downloading of data

Most systems, including DHIS2, enable staff to download data, but this could put client confidentiality at risk. PSI staff should be trained not to download individual client data without express authorization from their system administrator or M&E team. Ensure staff are aware of these restrictions and if they download data, that they use it only for authorized purposes.

✘ Don't allow data outside PSI without agreements in place

No individual client data should be shared with donors, partners, contractors or others unless a formal written agreement is in place to protect it. This agreement should impose security and confidentiality guidelines on the recipient. This agreement could be included in proposals.

Do…

✓ Get the message about client security out there

Ensure every staff member is aware of PSI's data security and confidentiality policies, and that user guidelines are posted next to every workstation. Don't just rely on passive dissemination – have staff actively sign an agreement, and reinforce this with training during other inductions or workshops.

✓ Build a culture of security and confidentiality

Ensure that every discussion about data, reporting or systems also covers security and confidentiality. Don't allow little slips here and there (e.g. a borrowed password to meet a deadline) as they send the message that these guidelines are flexible, which they are not. If you frequently discuss and strictly enforce security and confidentiality, a wider culture will gradually follow.

✓ Ensure all PSI equipment that stores data is secure

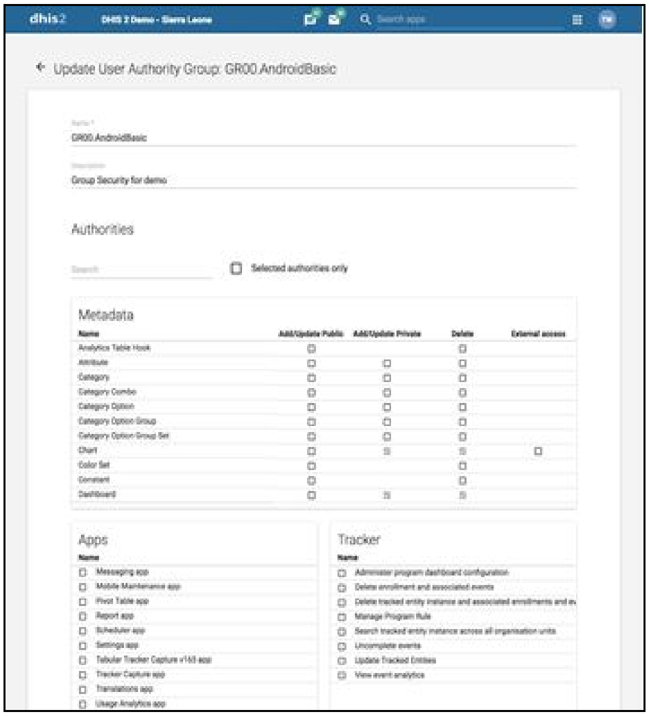
Data should only be kept on a PSI-controlled file sharing environment or on secure PSI equipment

- PSI laptops and mobile devices are encrypted;
- servers are kept in secure, locked rooms;
- staff use only encrypted mechanisms (e.g. PSI email addresses) for sending data;
- all backups are as secure as core data.

✓ Routinely audit your users

Staff who have left PSI must not have access to our systems. Ask your HR/payroll team for a weekly list of staff that have left or changed roles, and use this to adjust or remove users. Use features like DHIS2's "inactivity" search to identify users that have not logged in for two months or more and confirm this with line managers.

Creating an Android User



dhis2 DHIS 2 Demo - Sierra Leone

Search apps

Update User Authority Group: GR00.AndroidBasic

Name *
GR00.AndroidBasic

Description
Group Security for demo

Authorities

Search

□ Selected authorities only

Metadata

Name	Add/Update Public	Add/Update Private	Delete	External access
Analytics Table Hook	□		□	
Attribute	□	□	□	
Category	□	□	□	
Category Combo	□	□	□	
Category Option	□	□	□	
Category Option Group	□	□	□	
Category Option Group Set	□	□	□	
Chart	□	□	□	□
Color Set	□		□	
Constant	□		□	
Dashboard	□	□	□	

Apps

Name
□ Messaging app
□ Mobile Maintenance app
□ Pivot Table app
□ Report app
□ Scheduler app
□ Settings app
□ Tabular Tracker Capture v1.0 app
□ Tracker Capture app
□ Translations app
□ Usage Analytics app

Tracker

Name
□ Administer program dashboard configuration
□ Delete enrollment and associated events
□ Delete tracked entity instance and associated enrollments and ev
□ Manage Program Rule
□ Search tracked entity instance across all organisation units
□ Uncomplete events
□ Update Tracked Entities
□ View event analytics

Create Role
Before you can create a user, first you need to define a DHIS 2 user role. The DHIS 2 Android Capture App doesn't require any of the authorities that are encapsulated in a user role. The security for a DHIS 2 program or dataset is set as program or dataset data access.

For the purposes of web debugging problems with your users it is recommended that you create and assign a user role with data capture functionality, which should include:

- Tracker Capture app, Event capture app and/or Data Entry app
- Dashboard (to be able to login)
- Cache Cleaner (you will need to clean the cache)

Create user
Second, you should create a user, for which you will need to add some basic details such as the user name and assign it the role.

User Name: name.android
Example: belen.android
User Role assignment: assign to the role you created in step one.

Assign Organisation units

The third step is to assign the Org Units to the user you just created.

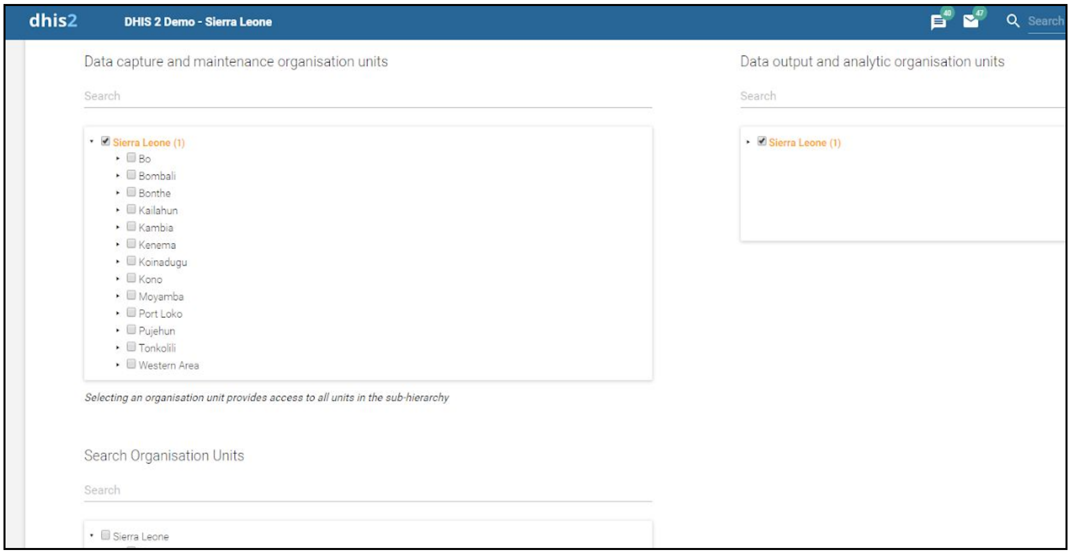
There are three types of organisation unit assignment:

- **Data capture:** Datasets and well as program creation of TEI, Enrollments and Events. Data pre-downloaded in the app at first login will be the one belonging to these org units.

  - Mobile users are not expected to access the org. unit hierarchy of a whole country. Maximum number of org units is difficult to set,as the App does not set the limit, but the resources on the device (memory, processor). We could say below 250 org units should be safe, but still believe that is a very big number for a mobile use case.

- **Data output:** for data analysis. Not applicable in Android.

- **Search Org. Units:** Expands TEI search (when online) across further Org Units. Individual records can be downloaded for offline use.
  - When configuring search org. units, make sure that your capture org. units are contained in your search org.units, to do that capture org. units have to be selected as well as search org. units.



Data capture and maintenance organisation units

Search

- ☑ Sierra Leone (1)
  - □ Bo
  - □ Bombali
  - □ Bonthe
  - □ Kailahun
  - □ Kambia
  - □ Kenema
  - □ Koinadugu
  - □ Kono
  - □ Moyamba
  - □ Port Loko
  - □ Pujehun
  - □ Tonkolili
  - □ Western Area

Selecting an organisation unit provides access to all units in the sub-hierarchy

Data output and analytic organisation units

Search

- ☑ Sierra Leone (1)

Search Organisation Units

Search

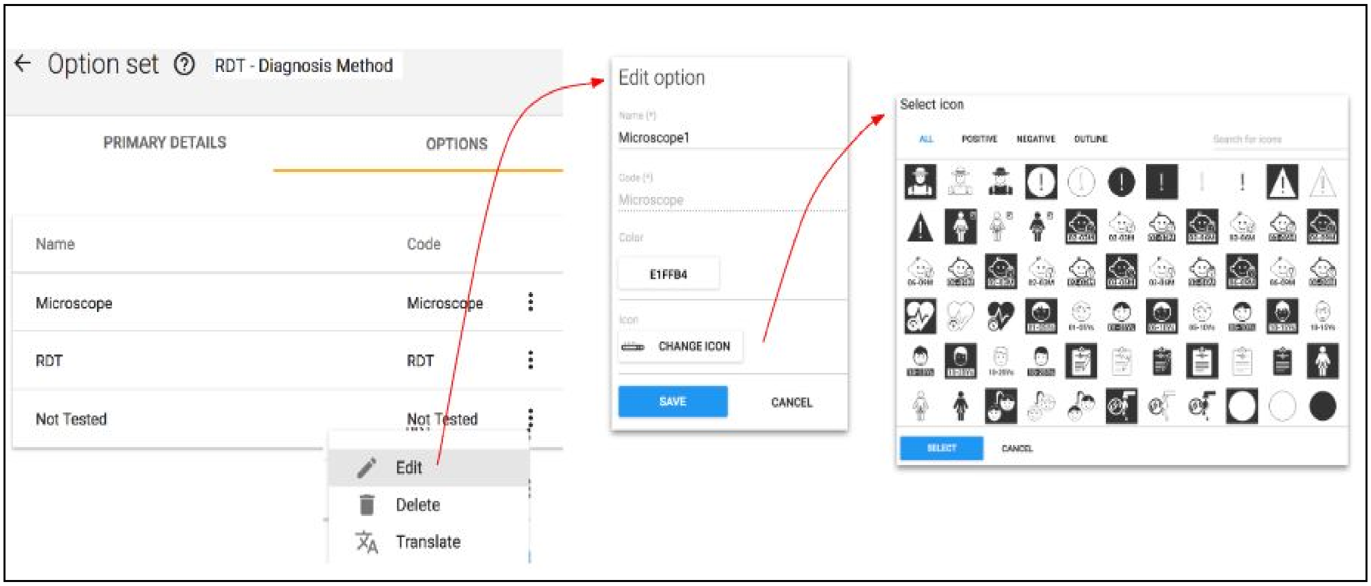
- □ Sierra Leone

Visual configuration: Understanding what renders and why

The information displayed and how it is displayed is configurable by the system administrator. There is an icon library of over four hundred images. The icons are assignable to most metadata objects: Options, Data Elements, Attributes, Programs / Data Sets. The images are not downloaded during the metadata sync process - only the icon name is downloaded. All icons already exist as highly efficient vector-based images in the APK of the app.

In the future you will be able to upload your own as gif/ jpeg/ png (50k or less - TBC). The disadvantage of this option will be the bandwidth use & syncing time, since the app will need to download images during metadata sync.

Here is an example of how to assign icons and colors to metadata:



Option set ⓘ RDT - Diagnosis Method

PRIMARY DETAILS | OPTIONS

Name	Code
Microscope	Microscope
RDT	RDT
Not Tested	Not Tested

Edit option

Name (*): Microscope1

Code (*): Microscope

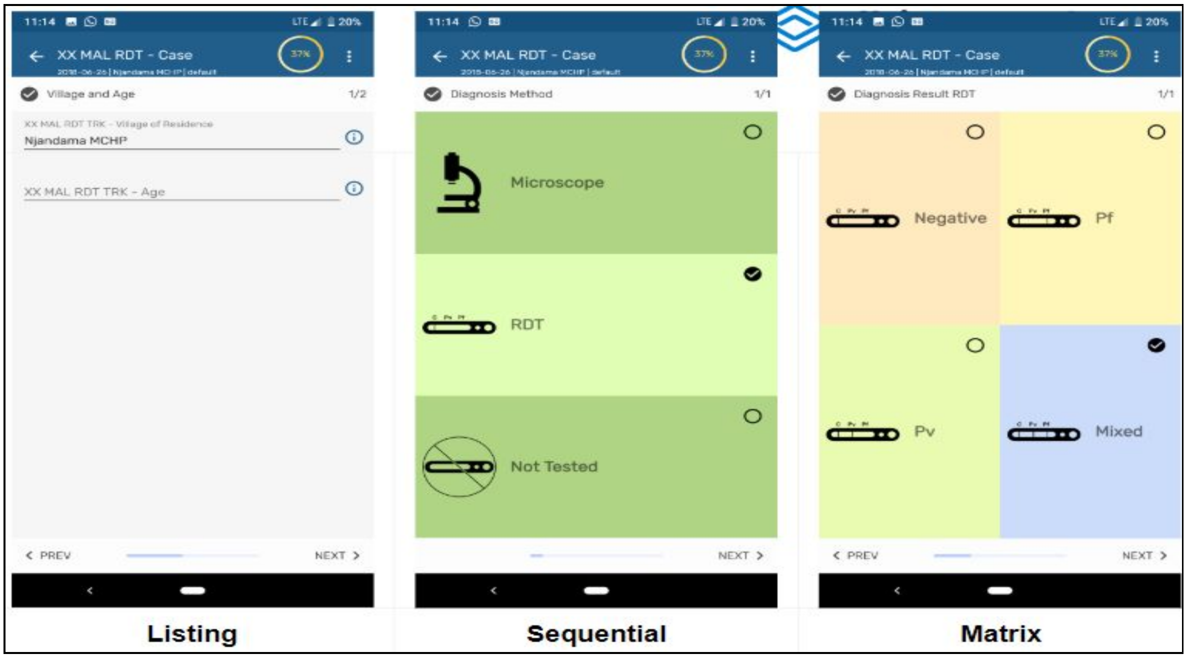
Color: E1FFB4

Icon: CHANGE ICON

The following table shows where you can use icons today:

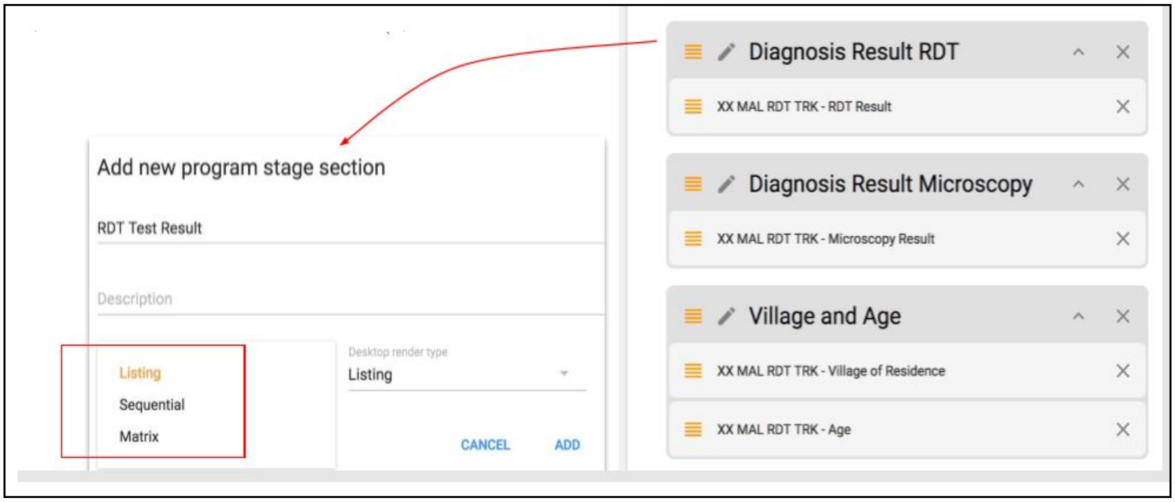
	Assign	Android Rendering	Web Rendering
TrackedEntityType	✓ 2.30	soon	
Program	✓ 2.30	✓	✓(simple events, 2.30)
Program Stage	✓ 2.30	✓	✓(simple events, 2.30)
DataSet	✓ 2.31	soon	
Data Element	✓ 2.30	-	
Attribute	✓ 2.30	-	
Indicator	✓ 2.32	soon	
Prg Indicator	✓ 2.32	soon	
Option Set	✓ 2.30	✓	✓(simple events, 2.31)

For program stages, sections can be rendered in three modes: Listing, Sequential and Matrix. The results of these modes are shown below:



Listing Sequential Matrix

A System Administrator can decide the best way to render the information in each program stage section by setting up the mobile rendering type, as shown on the screenshot below.


Add new program stage section

RDT Test Result

Description

Listing
Sequential
Matrix

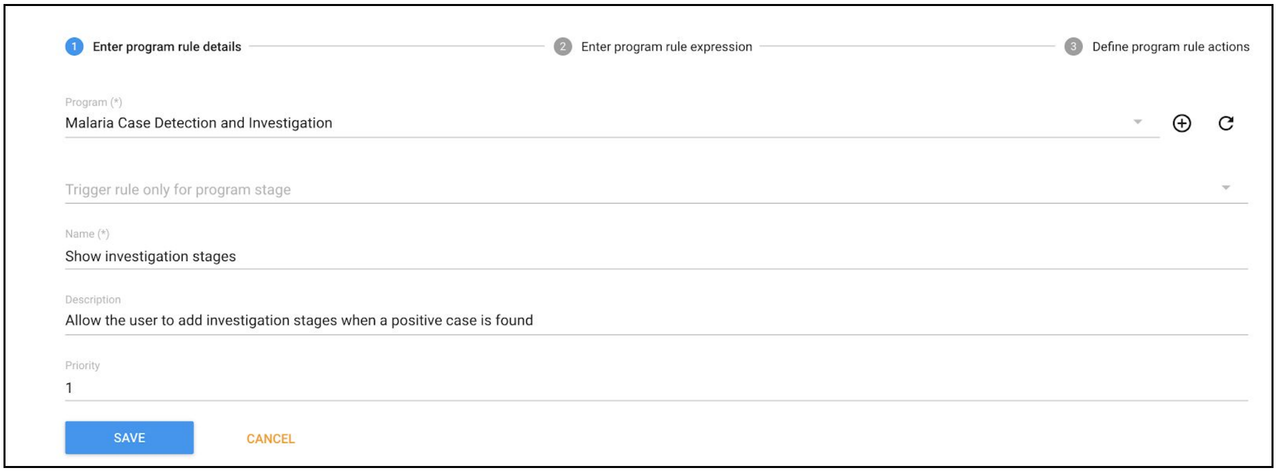
Desktop render type: Listing

CANCEL
ADD
Diagnosis Result RDT
XX MAL RDT TRK - RDT Result
Diagnosis Result Microscopy
XX MAL RDT TRK - Microscopy Result
Village and Age
XX MAL RDT TRK - Village of Residence
XX MAL RDT TRK - Age

Setting up the Program Rules

We recommend to test the Android App in parallel with the configuration of your program rules, this is to make sure that your changes in the server are properly reflected and working in the app.

The first thing you need to do when setting up the program rules is to define the context and priority for the execution of the rule. The context defines the execution of the rule for a specific program and optionally for a specific stage. The priority defines an order to execute the rules, this helps when the execution of one or more rules depends on the result of other rules.


1 Enter program rule details
2 Enter program rule expression
3 Define program rule actions
SAVE
CANCEL

Program (*)
Malaria Case Detection and Investigation

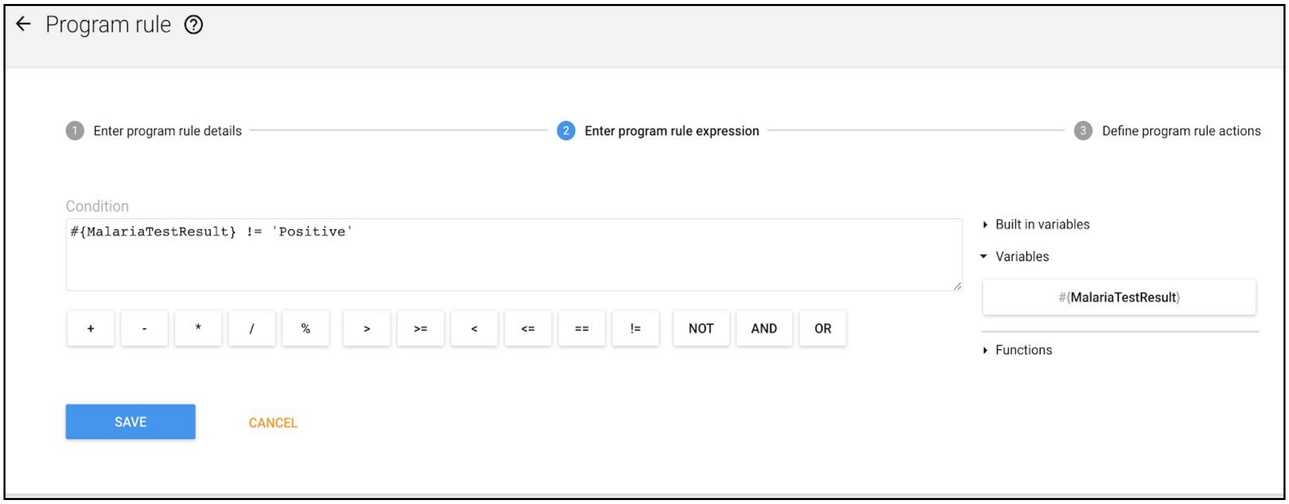
Trigger rule only for program stage

Name (*)
Show investigation stages

Description
Allow the user to add investigation stages when a positive case is found

Priority
1

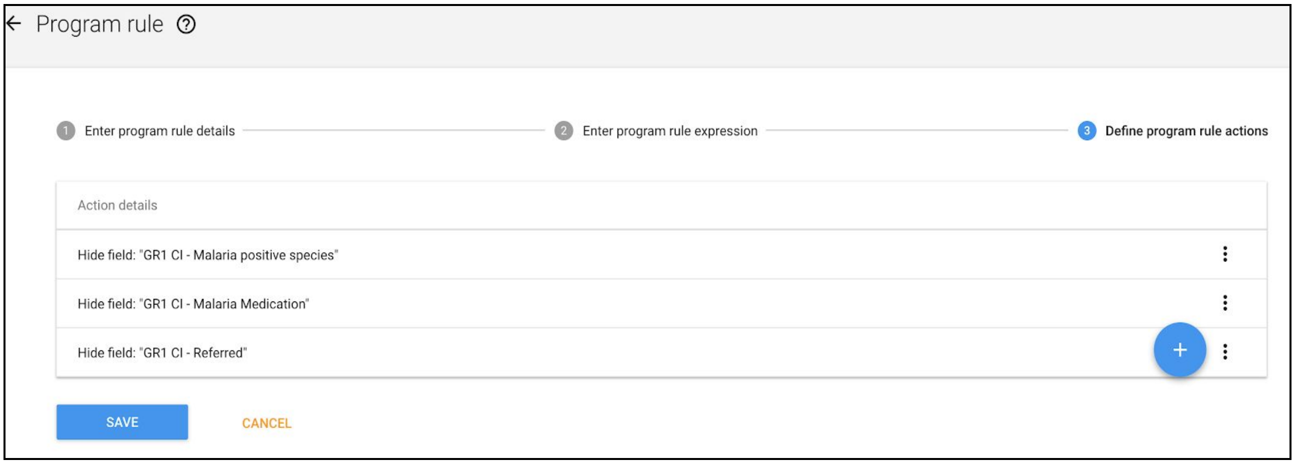
Once the context and priority have been defined, it is time to write the program rule expression using built-in variables, variables (TEI attributes / PS data elements) and functions. Variables have to be defined by the administrator to be able to evaluate information entered for a TEI attribute or a program stage data element.



Condition

```
#{MalariaTestResult} != 'Positive'
```

Then we need to decide on the action or actions to be executed when the program rule expression is true



Program rule

1 Enter program rule details — 2 Enter program rule expression — 3 Define program rule actions

Action details
Hide field: "GR1 CI - Malaria positive species"
Hide field: "GR1 CI - Malaria Medication"
Hide field: "GR1 CI - Referred"

When setting up your program rules you should be aware of what is supported by the DHIS 2 Android app. You can check the updated list in the complete documentation.

Defining Program Indicators and Legends

Indicators to be displayed in the App, can be calculated with the data from the Tracked Entity Instance (TEI) enrollment. Please keep in mind that calculations will apply in the domain of the TEI and the current Enrollment.

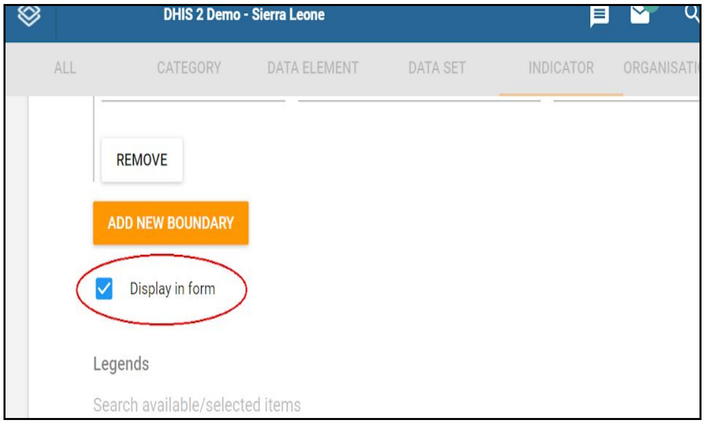
Aggregation types are not available, only Last Value can be used in the calculation of the indicator. All DE and constants can be used in the calculations. Variables are supported according to the following table:

Variables	
Event Date	✓
Due Date	
Incident Date	✓
Current Date	✓
Completed Date	
Value Count	✓

Variables	
Zero o Positive Value Count	✓
Event Count	
Program Stage Name	

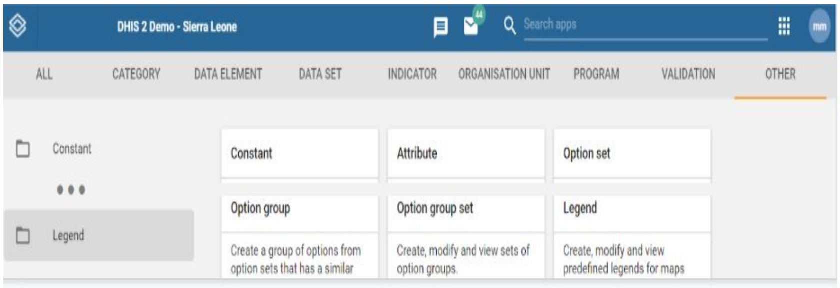
You can check the updated information of what is supported when using program indicators in the complete documentation. Analytic period boundaries are not supported, neither planned for future support, as they apply to multiple TEI’s.

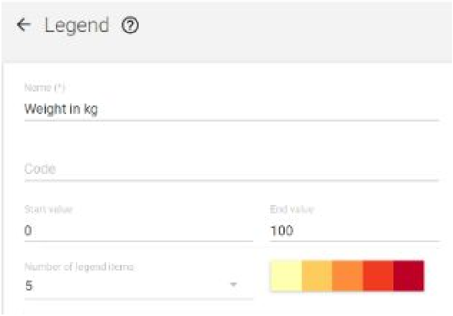
In order to display a program indicator in the App, you must select the checkbox “Display in form” in the DHIS 2 server indicator configuration wizard.



☑ Display in form

Once you have designed your indicator, you can assign a legend to it. In your DHIS 2 Server go to Maintenance > Others > Legends to create an new legend.


DHIS 2 Demo - Sierra Leone
Search apps
ALL
CATEGORY
DATA ELEMENT
DATA SET
INDICATOR
ORGANISATION UNIT
PROGRAM
VALIDATION
OTHER
Constant
Legend
Constant
Attribute
Option set
Option group
Option group set
Legend
Create a group of options from option sets that has a similar
Create, modify and view sets of option groups.
Create, modify and view predefined legends for maps



Name (*)
Weight in kg

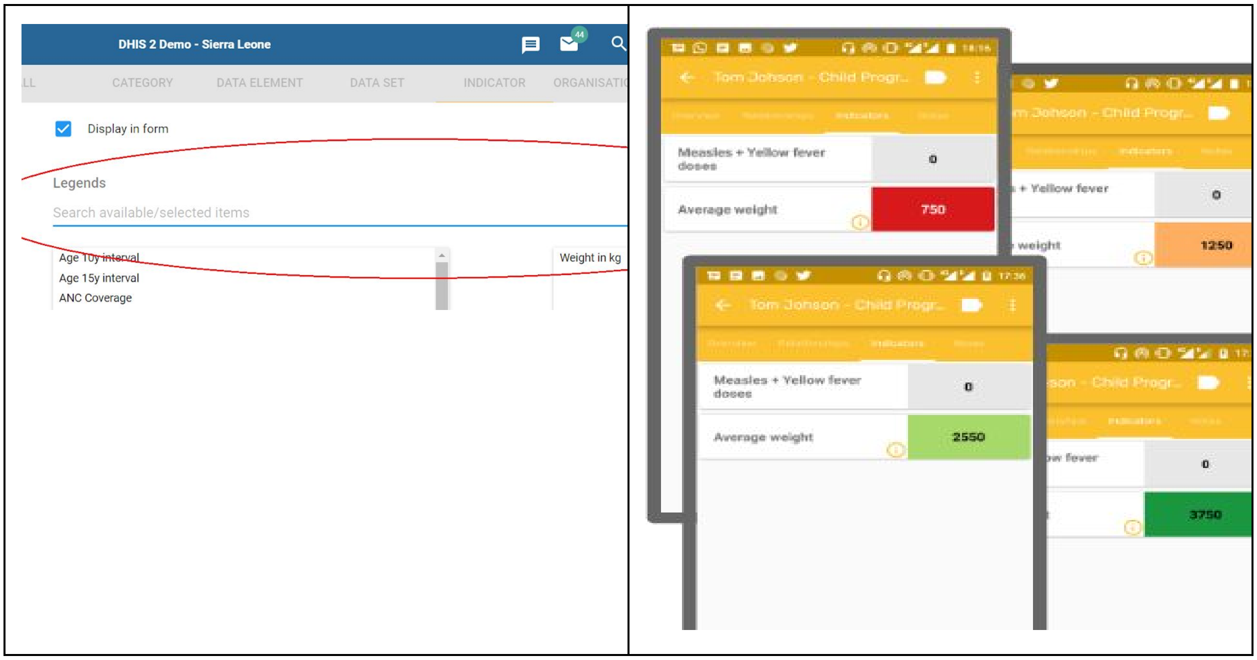
Code

Start value
0

End value
100

Number of legend items
5

Once you have created the legend you can assign it to the indicator. Alternatively, you can assign an already existing legend. Right underneath the checkbox to display the indicator in the App, you will find the section to search and assign the legend.



Reserved IDs

If you are working with tracker programs and you use auto-generated unique tracked entity attributes (see DHIS 2 documentation), it is important to understand how the app deals with the generation of values. Values are downloaded in advance from the server, so they are available when the application operates offline. Those values are marked as reserved on the server side.

When the user first syncs the app will download 100 values, which will be marked as reserved on the server side. From that point the user starts using the values as new tracked entity instances are created.

Everytime the user uses a value (registers a tracked entity instance), the app will:

1. Check if there are enough remaining values and refill when needed (if less than 50 values are available).
2. Assign the first available value to the tracked entity instance and remove it from the list of available values.

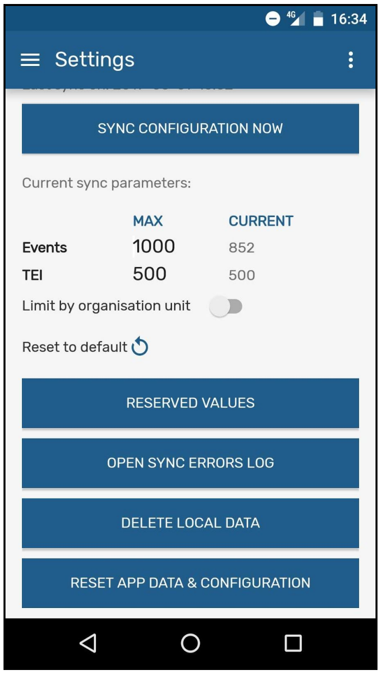
Whenever the app is synced it will:

1. Delete expired reserved values.
2. Check if there are enough remaining values and refill when needed (if less than 50 values are available).

A value is considered as "expired" when one of the following conditions is true:

- "expiryDate" is overdue. By default, the server sets the expiry period to 2 months.
- If the attribute pattern is dependent on time, i.e., it contains the segment `CURRENT_DATE(format)`, the app calculates an extra expiry date based on that pattern.

On the App, the user can also check the available values and refill them in the settings menu.



16:34

Settings

SYNC CONFIGURATION NOW

Current sync parameters:

	MAX	CURRENT
Events	1000	852
TEI	500	500

Limit by organisation unit

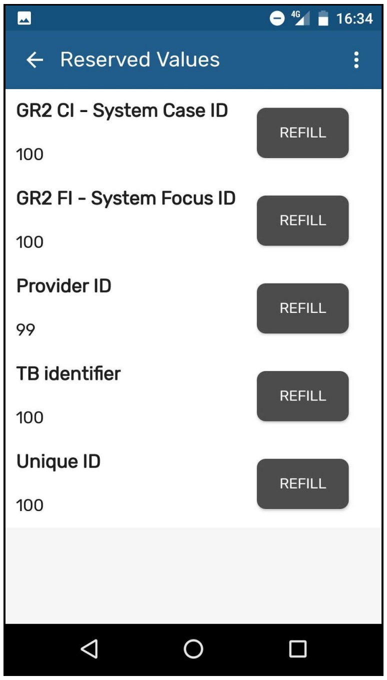
Reset to default

RESERVED VALUES

OPEN SYNC ERRORS LOG

DELETE LOCAL DATA

RESET APP DATA & CONFIGURATION



16:34

Reserved Values

GR2 CI - System Case ID	100	REFILL
GR2 FI - System Focus ID	100	REFILL
Provider ID	99	REFILL
TB identifier	100	REFILL
Unique ID	100	REFILL

When the app runs out of values and the server cannot provide more, the user will receive a message on the data entry form saying that there are no more available values. Your should fix that on the server side.

Installing the new DHIS 2 Capture App

There application can be downloaded and installed from two places:

- ❏ **Google Play** - This version does not allow screen broadcasting or taking screenshots.
- ❏ GitHub - There are two versions available in Github:
    - ❏ Production version: The same version than Google Play, it does not allow screen broadcasting or taking screenshots
    - ❏ Training version: With screen broadcasting and possibility to take screenshots (the one named with the suffix _training.apk)

    NOTE: when installing the training APK, you might need to allow 3rd party installs

Please read the section on App distribution for understanding the implications of using the different distribution channels.

Migrating from the old apps

Before you start with the installation of the new DHIS 2 Capture Android App in the field, it is important to note that if your users are already using the old generation DHIS 2 Android Event Capture or Tracker Capture, they should follow these steps:

1. Sync data of the current DHIS 2 app you are using
2. Download and install the new DHIS 2 Android Capture App
3. Login using your credentials.

NOTE: Deleting the app without syncing can cause information loss.

Login into the app

In order to log in you will need the DHIS 2 server URL, the user name and the password for the user you just created.For testing purposes you can also use the testing servers and credentials:

URL	user	password
Most recent DHIS 2 version: https://play.DHIS 2.org/android-current	android	Android123
Previous DHIS 2 version: https://play.DHIS 2.org/android-previous1		
Second previous DHIS 2 version: https://play.DHIS 2.org/android-previous2		

Testing

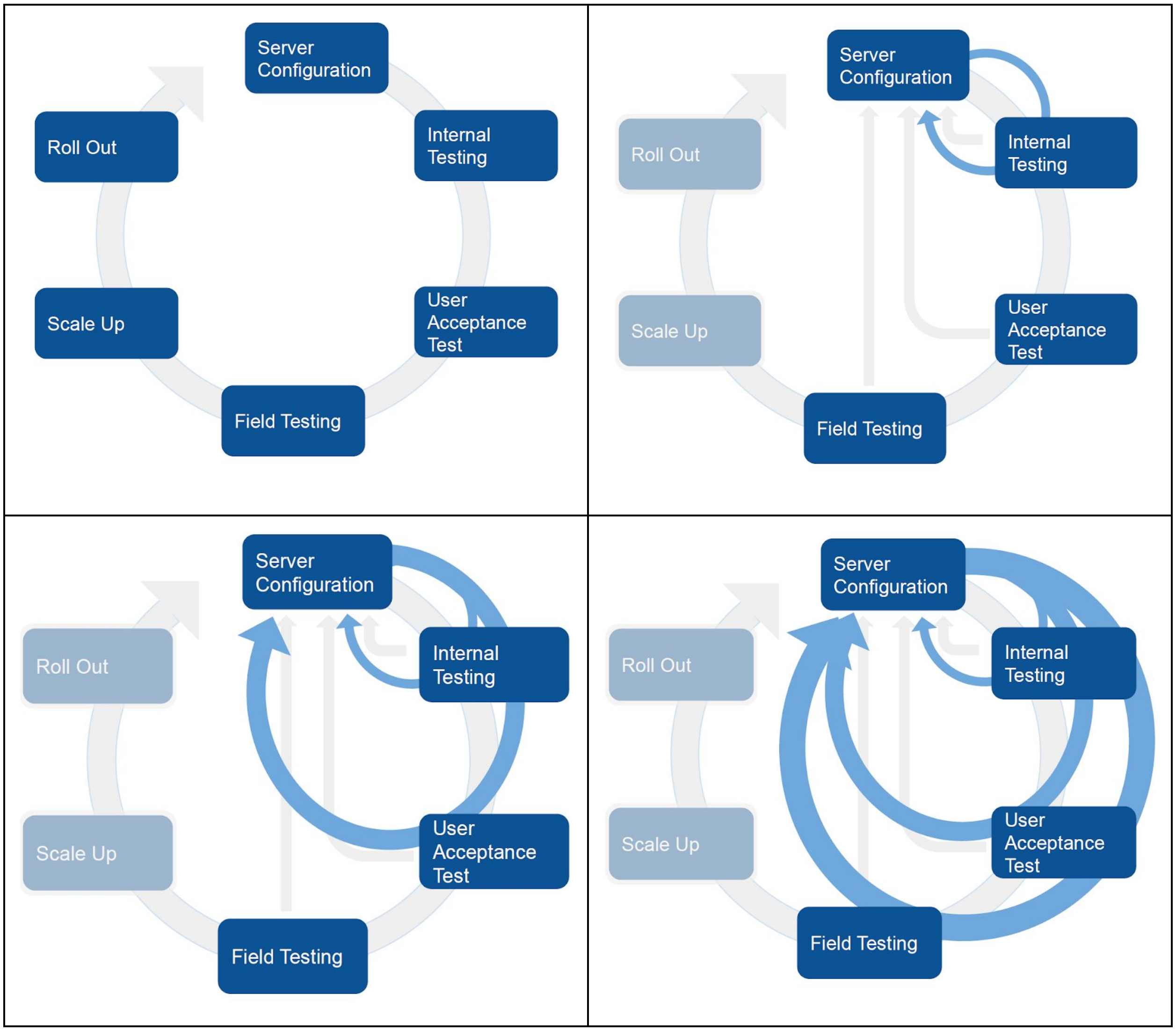
Now that the DHIS 2 server has been initially configured and you have installed the App in one or more devices, you are ready to start testing. While you are planning your testing you need to be aware of upcoming releases. It is important to be a part of the community at https://community.dhis2.org/ and use

jira, the software management tool that UiO utilizes. This will allow you to learn about the open issues in terms of features and bug fixing that it is scheduled for future releases.

We recommend to test the Android App in parallel with your configuration, to make sure that your changes in the server are properly reflected and working in the app. This is especially important during the configuration of the program rules. In addition to this step by step testing, there are different types of testing that you should conduct before rolling out the application.

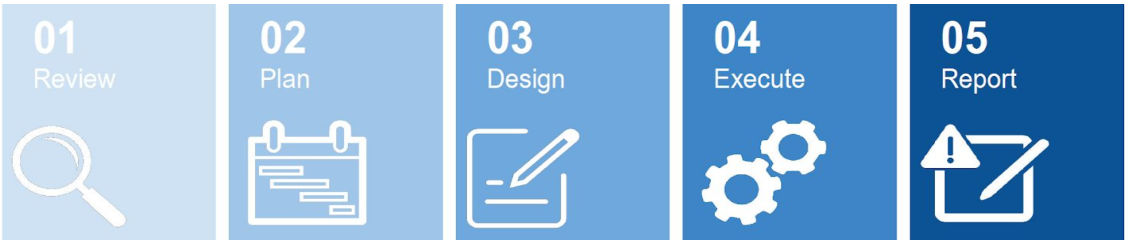
There is an initial set of tests that should be conducted internally with smaller groups to guarantee that the configurations are done correctly, that the functionality is in place and that the look and feel is adequate. As part of this initial phase of testing you will conduct what it is know as internal testing, followed by the UAT (User Acceptance Testing) testing. Later in this section we will elaborate on what these type of tests mean and how to conduct them. After that you will conduct your field testing and pilot. In this phase of the testing you will conduct a set of tests with larger groups to guarantee among other things that your workflows, your infrastructure and architecture is correct. Also later in this section we will elaborate further on these types of tests and how to conduct them.

The following graphs show that the next steps are iterative in nature, including new server configurations based on the results of the testing. You will most likely do several rounds of testing and reconfiguring before you are ready for scale up and roll out.



General Recommendations for Testing an Android App

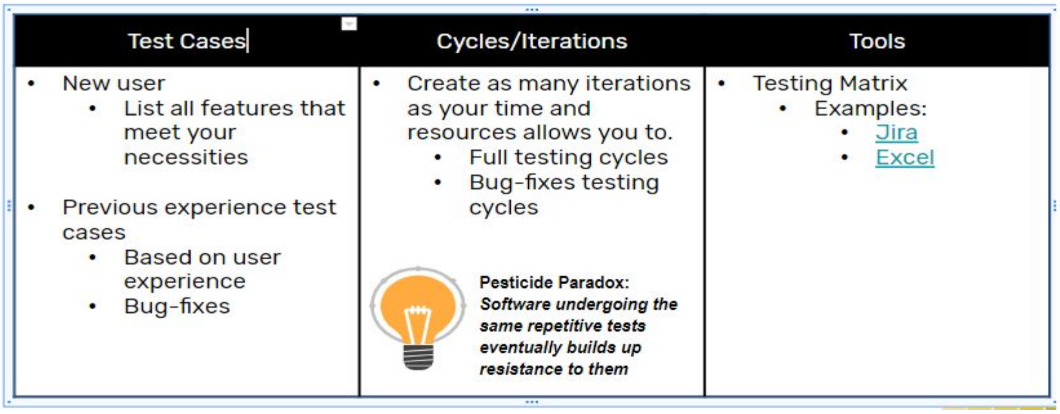
Before we go into the different testing phases, we are going to present some general recommendations that can be applied to testing an Android App. In general any process of testing can be summarized in the following steps:



1. **Review**. The first step is to review information about the application itself by going to https://www.DHIS 2.org/android-documentation. The documentation will provide you with information about the why's and what's or your testing. It should help you determine if the app meets your requirements, what the app can and can't do and help you analyze discrepancies. It should also help you identify new features and settings, features supported.

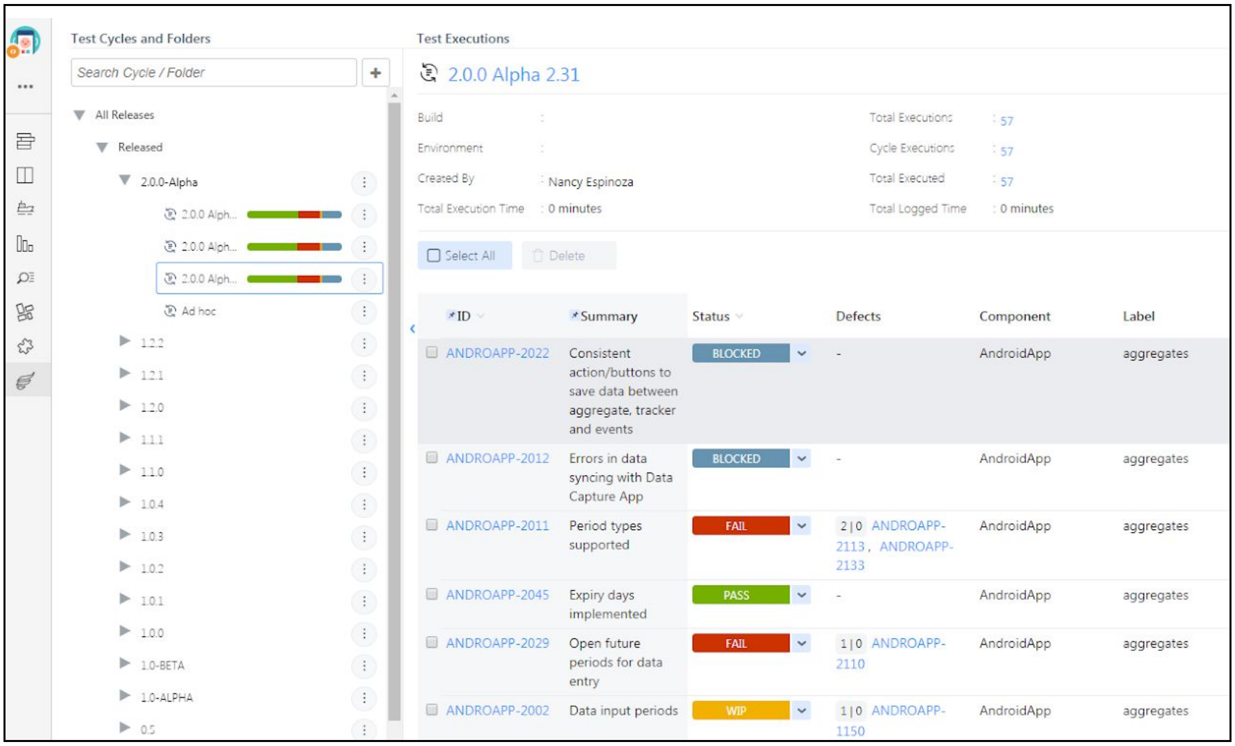
2. **Plan**. In this step you need to identify the time of testing by understanding the timeline for your own implementation. As part of this planning phase you must create a detailed list of requirements and classify them as compulsory (MUST have) or nice to have.

3. **Design**. In this step you must develop the test cases, decide the number of test interactions and the tools you will be using for your testing.



Test Cases	Cycles/Iterations	Tools
• New user • List all features that meet your necessities • Previous experience test cases • Based on user experience • Bug-fixes	• Create as many iterations as your time and resources allows you to. • Full testing cycles • Bug-fixes testing cycles **Pesticide Paradox:** ***Software undergoing the same repetitive tests eventually builds up resistance to them***	• Testing Matrix • Examples: • Jira • Excel

Example of testing tools - Jira



Test Cycles and Folders

Search Cycle / Folder +

- All Releases
  - Released
    - 2.0.0-Alpha
      - 2.0.0 Alph...
      - 2.0.0 Alph...
      - 2.0.0 Alph...
      - Ad hoc
    - 1.2.2
    - 1.2.1
    - 1.2.0
    - 1.1.1
    - 1.1.0
    - 1.0.4
    - 1.0.3
    - 1.0.2
    - 1.0.1
    - 1.0.0
    - 1.0-BETA
    - 1.0-ALPHA
    - 0.5

Test Executions

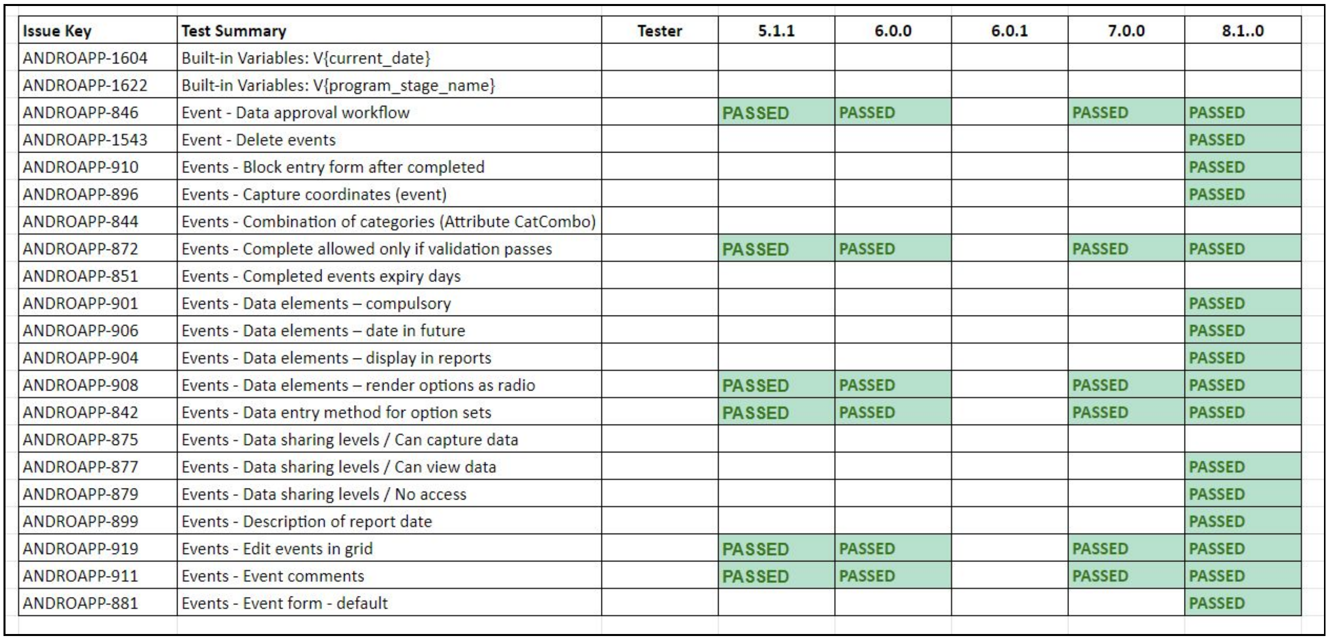
2.0.0 Alpha 2.31

Build	:	Total Executions	: 57
Environment	:	Cycle Executions	: 57
Created By	: Nancy Espinoza	Total Executed	: 57
Total Execution Time	: 0 minutes	Total Logged Time	: 0 minutes

☐ Select All Delete

ID	Summary	Status	Defects	Component	Label
☐ ANDROAPP-2022	Consistent action/buttons to save data between aggregate, tracker and events	BLOCKED	-	AndroidApp	aggregates
☐ ANDROAPP-2012	Errors in data syncing with Data Capture App	BLOCKED	-	AndroidApp	aggregates
☐ ANDROAPP-2011	Period types supported	FAIL	2 | 0 ANDROAPP-2113, ANDROAPP-2133	AndroidApp	aggregates
☐ ANDROAPP-2045	Expiry days implemented	PASS	-	AndroidApp	aggregates
☐ ANDROAPP-2029	Open future periods for data entry	FAIL	1 | 0 ANDROAPP-2110	AndroidApp	aggregates
☐ ANDROAPP-2002	Data input periods	WIP	1 | 0 ANDROAPP-1150	AndroidApp	aggregates

Example of testing tool - Excel



Issue Key	Test Summary	Tester	5.1.1	6.0.0	6.0.1	7.0.0	8.1..0
ANDROAPP-1604	Built-in Variables: V{current_date}						
ANDROAPP-1622	Built-in Variables: V{program_stage_name}						
ANDROAPP-846	Event - Data approval workflow		PASSED	PASSED		PASSED	PASSED
ANDROAPP-1543	Event - Delete events						PASSED
ANDROAPP-910	Events - Block entry form after completed						PASSED
ANDROAPP-896	Events - Capture coordinates (event)						PASSED
ANDROAPP-844	Events - Combination of categories (Attribute CatCombo)						
ANDROAPP-872	Events - Complete allowed only if validation passes		PASSED	PASSED		PASSED	PASSED
ANDROAPP-851	Events - Completed events expiry days						
ANDROAPP-901	Events - Data elements – compulsory						PASSED
ANDROAPP-906	Events - Data elements – date in future						PASSED
ANDROAPP-904	Events - Data elements – display in reports						PASSED
ANDROAPP-908	Events - Data elements – render options as radio		PASSED	PASSED		PASSED	PASSED
ANDROAPP-842	Events - Data entry method for option sets		PASSED	PASSED		PASSED	PASSED
ANDROAPP-875	Events - Data sharing levels / Can capture data						
ANDROAPP-877	Events - Data sharing levels / Can view data						PASSED
ANDROAPP-879	Events - Data sharing levels / No access						PASSED
ANDROAPP-899	Events - Description of report date						PASSED
ANDROAPP-919	Events - Edit events in grid		PASSED	PASSED		PASSED	PASSED
ANDROAPP-911	Events - Event comments		PASSED	PASSED		PASSED	PASSED
ANDROAPP-881	Events - Event form - default						PASSED

Every test case should include the following sections. The level of detail and the content of the test to be performed will depend on the level of experience-profile of the user.

❏ Identification: Cycle number / ID, Test ID, version, test summary.

❏ Description: details, steps to reproduce

❏ Status report: Date of execution, executed by, expected vs actual result, execution status report ID.

4. **Execute**. During the execution of your testing please keep in mind two important issues:

❏ Metadata Configuration: Verify the program settings on the web and check the documentation to know the behavior of the features in the app. This will help to identify true bugs versus problems derived from the configuration or unsupported features.

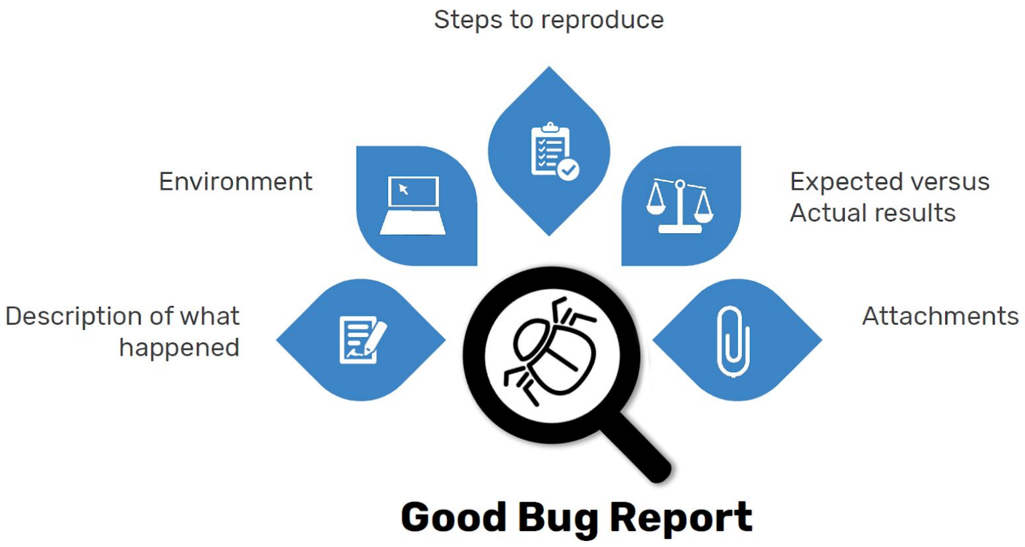
❏ Matrix of Completion: Check your progress according to the deadlines you have designed in the plan stage. Also make sure notes are being taken rigorously to be able to report a bug.

5. **Report**.There are three important characteristics that your report must have

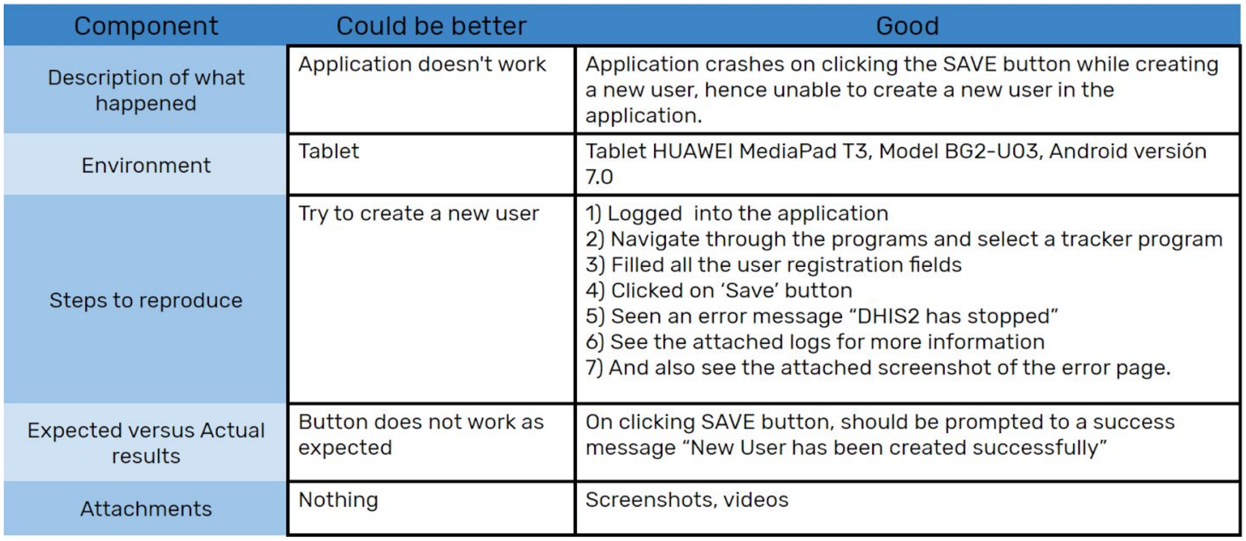
❏ The reported error must be reproducible

❏ The information must be specific and informative

❏ The report must separate facts from speculations



The table below summarises a good Bug Reporting with some examples:



Component	Could be better	Good
Description of what happened	Application doesn't work	Application crashes on clicking the SAVE button while creating a new user, hence unable to create a new user in the application.
Environment	Tablet	Tablet HUAWEI MediaPad T3, Model BG2-U03, Android versión 7.0
Steps to reproduce	Try to create a new user	1) Logged into the application 2) Navigate through the programs and select a tracker program 3) Filled all the user registration fields 4) Clicked on 'Save' button 5) Seen an error message "DHIS2 has stopped" 6) See the attached logs for more information 7) And also see the attached screenshot of the error page.
Expected versus Actual results	Button does not work as expected	On clicking SAVE button, should be prompted to a success message "New User has been created successfully"
Attachments	Nothing	Screenshots, videos

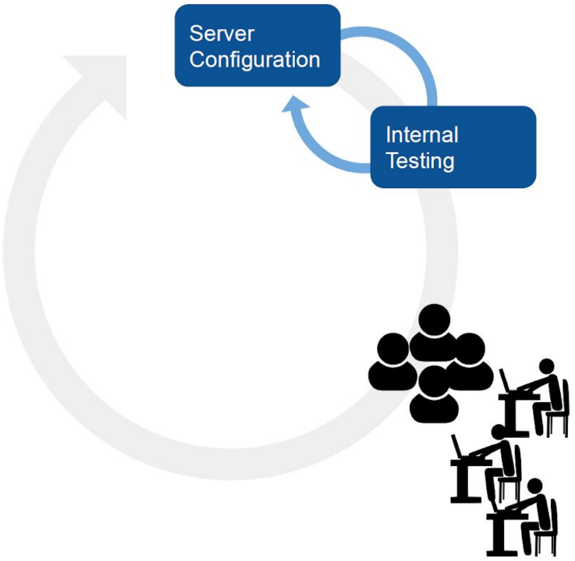
Internal testing and UAT testing

What are you testing

You are testing your DHIS 2 server configuration and the Android App itself.

What are you looking for?

Program Rules, forms, visual UI, indicators… Bugs, improvements, new requirements, etc.



How?

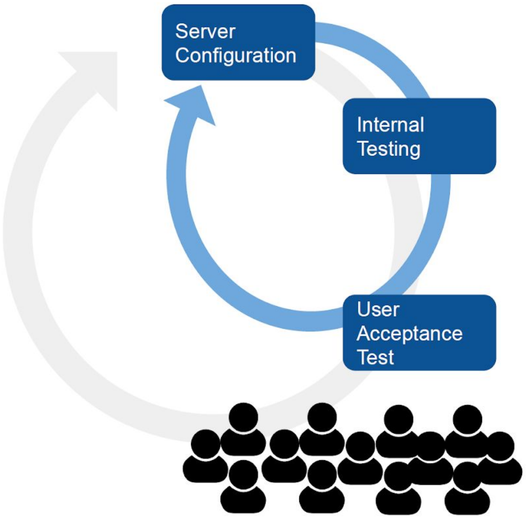
Methods and periods for testing vary from group to group, but it has to be iterative, flexible and it must be done in the early stages of the deployment process. You need to spend time deciding who will participate in the test, develop a test plan and have a strategy to gather the feedback. There are different tools available to report and track bugs and issues. Depending on the complexity of your test you can use trello, jira,etc.

Setting the right foundation for your internal testing will increase the quality and the efficiency of the testing sessions. These recommendations apply to any of the different tests that you will need to perform.

UAT Testing

What are you testing

You are testing your system configuration (input), your visual UI and icons, usability and your outputs. You can also test at this stage the user experience with different devices (smartphone, tablet, external keyboard, chromebook).



What are you looking for?

Adjustments in the previous items and hardware issues. This is a good time to start identifying champions that will help on future phases. The main purpose of the UAT is having people from different background in agreement with the configuration to execute the field testing. The success of this stage will determine move to the next phase, field testing

How?

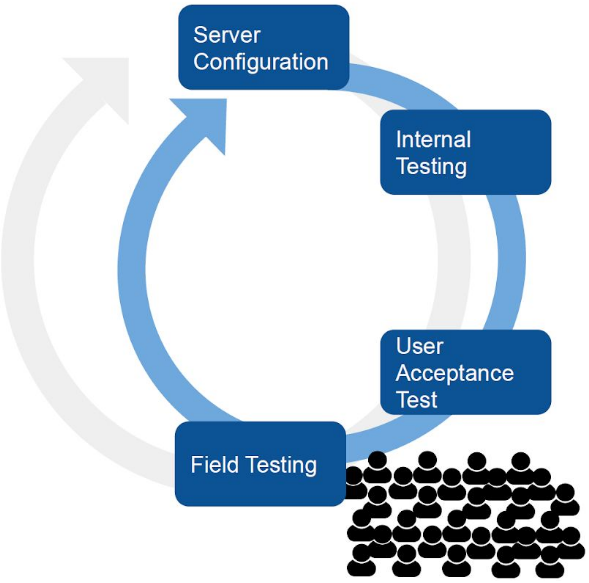
Use a controlled environment. Find users with little exposure to the technology, who are not necessarily integrated in work practices. Your users could be: 1) Expert in the health area/s, 2) Field officer, 3) Field user.

The size of the group will vary depending on the type of project you are implementing the App for. An average size UAT test group would be between 5 and 10 people.

When deciding who will participate in your test, think about all the different types of users and their roles. With that in mind, select your testers. You should provide your testers with the right onboarding and guidance. They need to be well informed of the methods you will be using for testing, the expectations and the overall objectives and goals of the testing. It is advisable, if at all feasible, to organize testing sessions with one or two leaders, where testers can help each other and have the possibility to ask questions and get help in the spot from the leaders.

Another important aspect to consider is test data. You must have enough data in your test server to allow for the testing of different test cases.

Field Testing/Pilot



What are you testing

You are testing your SoP's and workflows.
You are testing your infrastructure/architecture.
You are testing the different devices.
You are testing your training procedures & materials.

What are you looking for?
Adjustments in the previous items.
Suitability of the selected devices for the work space and environment.
Evaluate your solution
Identify champions.

How?
20-30 users. Recommended 2 months (plan ahead!). Decide distribution (locations). Do not pick the easiest or the most complex. Keep it simple but challenge your solution.

Considerations for evaluating your pilot

You should define your indicators for evaluating your results and decide your strategy for piloting your system You could use your current system and the new system in parallel for a few months or simply replace it. Both strategies have advantages and disadvantages and you should analyze them carefully with your team before pilotin.

Some advantages of having the current and new system in parallel are:

- you can have evidence on how the new system improves in comparison with the old one in terms of timeliness, or data quality for example, this parameters depend on the purpose of your specific project.
- You have your previous system as backup mechanism if something does work as expected
- Builds trust on the users when they compare both results.

Some disadvantages are:

- You are setting a double-reporting mechanism, it duplicates the time and level of effort from your users. IT is important to handle this with sensitivity and prepare potential support human resources when needed.
- The possibility of users to compare both systems in parallel could be a double edged sword, as users tend to resist change.

Scale Up

Acquisitions

Now that you have performed all your testing and your pilot project, you are ready to scale up your deployment, for which you will need to do acquisition of Hardware and necessary services. You will need to make decisions regarding:

❏ Purchasing of devices vs BYOD (bring your own device)

❏ Distribution of the app (now and later)

❏ Telecommunication contracts

Purchasing of devices vs BYOD (bring your own device)

Initially you should buy different devices to allow users to evaluate them and provide you with feedback. Once the device that you will be using is decided upon, you should only buy 10 or less units, or whatever is needed for the testing and the pilot phases. Only when the pilot is coming to completion, you should buy equipment for the next 6 months roll-out. Some very large projects will take years for a national roll-out, and your hardware adquisicion plan should expand across years. Recommendations on the technical specs for devices are in the chapter ‘Technology Requirements’.

You should consider the feasibility of using a BYOD policy - this format allows users to bring their own devices, as long as they satisfy a minimum technical standard, which you will define for your project. You will normally offer some sort of incentive, likely to be in the form of eCash or airtime. The advantages of this approach are obvious: it avoids the large initial cost for acquisition, as well as it reduces the administration costs and logistics considerations. On the other hand, you will have the challenge of a very heterogeneous hardware environment, meaning different devices and Android OS versions. This mainly affects the debugging process.

Distribution of the app (now and later)

DHIS 2 Android app has a new release every couple of weeks. Each new release contains bug fixes and could contain new functionality. It could also contain new bugs. New versions are published in GitHub as well as Google Play store. Github is only a repository: you will download a specific APK and install it on your device. You will need to allow the use of third-party permissions to install an APK. Once an APK downloaded from GitHub or via other method, the installed version will never auto-update. On the other hand, if you install from Google Play, it normally auto-updates to the latest version. It is possible to disable auto-update in gPlay if you need to.

Once you complete your testing and training materials, and start your rollout, you don't want the application version to change for any of the users, unless you have re-tested the new version. Version changes could include a modified UI, erroneous behaviours, or an incompatibility with your DHIS 2 server version. You want to thoroughly test new versions before pushing them to your users, so you can ensure that the new version doesn't cause any problems to your configuration, requires retraining, on requires changes to your configuration.

In summary, for any installation that involves a significant number of devices you should avoid the use of Google Play, and instead use a Mobile Device Management (MDM) solution, which we discuss in this chapter. If you don't have access to this option, you could consider using Google Play, but you should disable auto-update for the DHIS 2 android application. The procedure on how to do this changes by Android OS version - please google 'how to disable android auto update by application in Andrid X.X'.

Telecommunication contracts

If your installation plans to include the use of SMS for transmitting selected records via SMS when mobile data is not available, you will need to establish a contract with a local aggregator which can provide you with an incoming number to receive the SMS. You should configure your server to receive & send SMSs - please see DHIS 2 documentation on SMS connections. You will need to estimate the number of messages per month to be able to forecast the monthly cost.

The process of selecting and signing a contract with an SMS provider varies by country and it depends on the procurement procedures of your organization.

Mobile Device Management

Mobile Device Management refers to software used for the administration of mobile devices. You will need an MDM software when you have to support hundreds of devices and it becomes necessary to control the apk file distribution across the devices, provide tech support and enforce institutional policies. Most options are offered as monthly-fee services. Some free apps offer kiosk mode, but charge a monthly fee for basic remote management.

The desirable features of an MDM software can be classified as basic and advanced. Here is a list of the desirable features:

- ❏ Basic features:
  - ❏ Require a screen lock password
  - ❏ Provision of authorized apps
  - ❏ Lock devices and wipe information if they're lost or stolen
  - ❏ Control the upgrade of the Android App
  - ❏ Enforce backup policies
- ❏ Advanced features:
  - ❏ Enforce password strength policies
  - ❏ Enforce network usage policies
  - ❏ Track device location
  - ❏ Restrict access to settings and features (example - wifi/network, screen capture)

When deciding which is the best MDM software for your needs you should try to answer the following questions:

- ❏ How many devices do I need to manage?
- ❏ How often do I have physical access to the device?
- ❏ Which features do I really need?
- ❏ Which policies do I have to implement
- ❏ How hard will it be to install and maintain
- ❏ How will it affect the user experience?
- ❏ Do we need to allow BYO? (Bring Your Own Device).
- ❏ How will it affect the device?

In the next page you can find a list of available MDM software (please keep in mind that prices and conditions will change over time).

Mobilock Free (unable to update software)
SOTI (MobiControl) (can be expensive - $2.20/device/month)
Miradore (no remote support)
Applock (unable to control software update)
AcDisplay (unable to control software update)
F-Droid (unable to limit data consumption)
APPDroid (unable to limit data consumption)
Master List (unable to control software update)
Firebase (unable to limit data consumption)
Intunes (users need to be part of a MS Office 365 deployment)
MobileIron (can be expensive - $3.15/device/month + $2,368 for deployment)
IBM Maas360 (too expensive - $1.60/device/month + $0.50/device/month for remote support, for 3,000 devices)
AirWatch (unresponsive and can be expensive - $3.80/device/month for 3,000 devices for 3 years)
XenMobile (Citrix) (can be expensive - $2.03/device/month for 3,000 devices)
Good for Enterprise (Blackberry) (can be expensive - $2/device/month + $2.5K for deployment)

Training

An important step before roll up, is the training of the users and if necessary, the training of the teams providing support to the users. There are many training strategies that you can follow and it will depend on the size of the group that needs to be trained, their skill level, the time frame available, the budget, etc. It is important that you put time and energy into designing your training strategy and allocate enough time to accomplish your training goals. Having your users well trained and informed will reduce user's anxiety and adoption problems and it will also increase the quality of the data collected.

Technical Preparations for the Training

When preparing for the training, ensure that all the practical technical requirements have been met. This includes having the tablets/mobile devices ready, with the new DHIS 2 Capture Android Application installed. Depending on the availability of internet connectivity at the area where you will be performing the training, you might have all the tablets pre-synched with the server, so that you have enough data and the right configuration for the training.. Before doing the training, the exercises should be tested to ensure everything is working. Troubleshoot issues detected during testing so they do not arise during training. You may want to do a second round of the test to spot any issues missed in the first round.

If the training is done with pre-synched data and configuration, at the end of the training, make sure to let the trainees experience the App accessing the DHIS 2 remote server. This will give the trainees the possibility to experience real-life sync experience, which may include delays in the network. Without experiencing delays, they may later interpret network delays as faults in their device.

Training Budget

Following, there are some guidelines on preparing the budget which are taken from the DHIS 2 Community Health Information System Guidelines document published by the University of Oslo:

- ❏ Follow organizational policies in using approved budget templates and rates (indirect, DSAs, etc.) for all expenses including:
  - ❏ Travel (e.g. fuel, car hire, lodging)

    - ❑ Personnel (e.g. per diems, meal costs)
    - ❑ Venue (e.g. conference space, tea breaks)
    - ❑ Materials (e.g. printing, hardware, projectors)
    - ❑ Miscellaneous items

- ❑ Build budget based on in-sheet calculations of materials needed, unit cost of that material, and number of units needed. You can also build in additional multipliers to illustrate number of units per attendee. This allows flexibility in updating the budget if unit costs change, or number of participants increases or decreases.
- ❑ Budget anticipated expenses in local currency, with a conversion rate built in (that can be updated as needed) to convert to the desired currency of your organization or funder.(2).

Training Agenda

The DHIS 2 Community Health Information System Guidelines document written by the University of Oslo recommends that you consider:

1. The type of seating you require (round table, individual desks, etc.).
2. Technological requirements (computers for all, Wi-Fi bandwidth, etc.),
3. Finance for conference center allowances, participant food and beverages
4. Trainers need space to walk around to observe and help each participant.

Be aware of the number of attendees you expect at each training, as providing sufficient materials and space will be necessary. Event space should be large enough for the group and also appropriate for the planned activities.

Training Materials

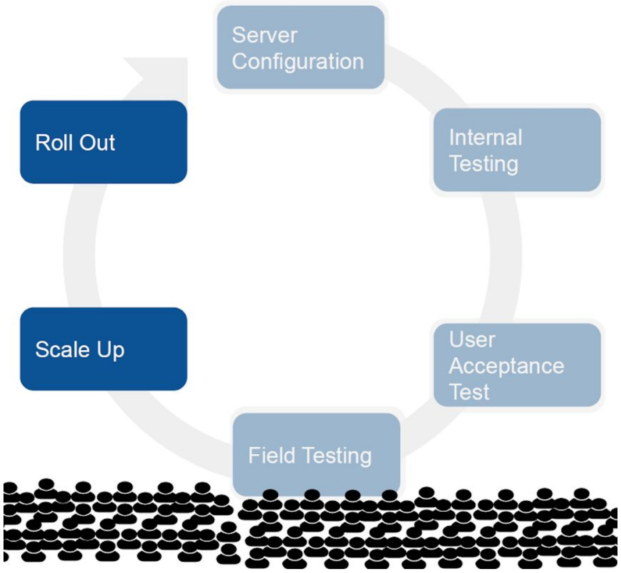
In the same document we find recommendation for the training materials as well, which we include here. The materials you will need for your trainings will depend on your activities. To ensure you are planning for everything, walk through your training agenda with a partner, and discuss what will be done for each part of the training, taking note of the materials needed.

The agenda for training sessions should be defined well-ahead of the training and included in materials distributed.

User documentation should be packaged in Minimal Manuals. These manuals explain a specific work task (e.g. enter monthly data from village health register or compare health in your village with the neighboring villages). After explaining the work task, the Minimal Manual provides numbered step-by-step instructions with screenshots, so that users recognize what to do. Keep in mind that Minimal Manuals do NOT explain the functionality of the app, one by one, like a typical vendor user manual. Since users prefer doing and not reading, the manuals should be a short as possible while still containing all steps.

Rollout

At this stage you should be ready to roll out the devices and the App to your end users. In this step you will have to prepare for the cut-over and coordinate the go-live, you will need to decide if you will keep parallel systems in case you are using other Apps or do a straight replacement. As far as paper and manual processes go, you will also need to decide if you want to eliminate them, replicate them or keep a duplicate. Make sure you pick carefully the time to go live. Pick a time where teams will be available to spend the extra time and effort adapting to using the new App and also make sure extra support is available during the initial stages.



Following we include recommendations for this phase of the implementation from the DHIS 2 Community Health Information System Guidelines document written by the University of Oslo.

The end users of the newly rolled out App, should have one point of support. Ideally their supervisor can provide this one point of support. Since users know their supervisor and get support for other issues, having the supervisors supporting the App is an advantage.

You might already have in place a multi-tiered support system for the web based DHIS 2 and perhaps you can use it to also provide support with the App. Multi-tiered means simple issues are able to be addressed by lower level supervisors and more difficult or complex issues are move up the tiers until they reach someone who is able to address them. The vast majority of issues requiring support will be simple issues that should be able to be addressed by the first tier of support. Often this first tier is the user's direct supervisors. This tier should be able to address simple hardware and software issues. If the supervisors cannot resolve the issue that will then have to escalate it to a higher tier. Tier Two requests are often addressed by district level or sub-national information systems officers, who are trained to manage system configuration issues and all advanced issues around the user interface, data imports and exports. Tier Three requests are typically addressed by central level IT support persons. They should be able to respond to any back-end maintenance requests.

The number of tiers of support might vary based on the complexity and size of your project. Regardless of the number of tiers, it is essential that support requests can be submitted by any user directly through either the web, phone or by email. Once a request for support has been sent to the technical team should acknowledges receipt of the request within a short time period like 12 hours (2).

By now you should have a plan on how you are going to keep track of the devices you are handing out to your teams. Here are some best practices you might want to follow when tracking devices (2):

- ❏ Number each phone (tablet) box and two copies of the phone agreement (i.e. #1 on a box and on both agreement forms) and hand both to a community health worker supervisor to fill in the forms against the details of that phone.
- ❏ Ensure that the phones and boxes do not get mixed up.
- ❏ Collect the agreement forms, and have a council sign and stamp both copies. One copy will remain with the district, and the other will be returned to the partner and kept in the district box file in the office.
- ❏ Use a QR code generator to generate a QR code with the phone's information (number, CHW, SIM number, district, etc.). You can then print this QR code onto a heavy-duty label sticker and apply the sticker to the back of the phone or inside the phone in the battery compartment.
- ❏ If providing SIM cards with phones, document the associated SIM card and phone.
- ❏ To prevent tampering of the SIM card is provided with the phone, glue the SIM into the phone by placing the SIM card in the phone and applying glue to the back.

You should also reflect on Device Ownership and Usage. Right at the time of giving the devices (phones, tables, etc.) to the users, it is important to clarify the ‘ownership’ of the devices along with the responsibilities of maintenance, upkeep and loss. There is often confusion on whether the device is owned by the institution or the individual, and what the respective responsibilities are. However, if the end users are expected to use personal devices, it is all the more important to clarify issues on airtime/data cost along with the reimbursement mechanism (2).

Mobile Implementation Checklist

Task	Completed
Analysis of Technology Android App and Server Requirements	□
Strategy for Data Security and Privacy	□
DHIS 2 Server Set Up and Configuration	□
DHIS 2 Server Instances	□
Data Elements, Option Sets, Programs...	□
Visual Configuration	□
Defining Program Indicators and Legends	□
Setting up the Program Rules	□
Creation of Android User	□
Sharing Settings and Security considerations	□
Installation and App Setup	□
Installing the App	□
Login into the App	□
Testing	□
Internal testing	□
UAT testing	□
Field Testing / Pilot	□
Pilot	□
Scale Up	□
Hardware acquisition	□
App Distribution Strategy	□

Mobile Device Management Strategy	□
Telecommunication contracts	□
Task	**Completed**
Training	□
Technical preparations	□
Budgeting	□
Agenda and Participants	□
Materials	□
Roll Out plan	□