SOP for the Operation and Management of the Ideal Health Facility information system

July 2023

health

Department:
Health
REPUBLIC OF SOUTH AFRICA

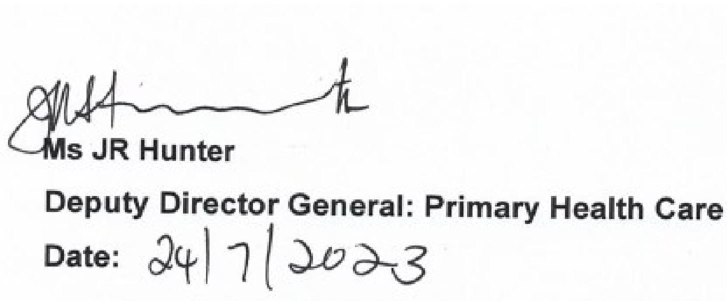
This standard operating procedure sets out the operation and management of the Ideal Health Facility web-based information system located at https://www.idealhealthfacility.org.za/ .

Revision of the SOP is done when:

- a new service provider is appointed/contract is renewed
- additional modules are added
- functionality of modules is changed
- management of the information system is changed

Summary of SOP version controls:

Date updated	Description of updates
April 2018	
December 2019	Complete overall of the SOP.
June 2021	User account lists and review of user accounts.
October 2022	System environment, maintenance and security of user accounts.
July 2023	Password configuration, NDoH service desk for end user, Service desk requests for service provider, training and disaster recovery plan.



Ms JR Hunter

Deputy Director General: Primary Health Care

Date: 24|7|2023

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ANNEXURES

1. Introduction

The Ideal Health Facility (IHF) web-based information system is located at https://www.idealhealthfacility.org.za/

The Ideal Clinic Realisation and Maintenance (ICRM) programme was initiated by the National Department of Health (NDoH) in July 2013 in order to systematically improve quality of care provided at primary health care (PHC) facilities. In October 2014 the programme was incorporated into the Presidential Operation Phakisa programme that assisted the NDoH to develop a detailed implementation plan for scaling up ICRM. To monitor the progress of this programme, an information system was developing. The Ideal Health Facility information system was developed in 2013 and rolled out to all provinces in 2015. The information system had one module to capture the quality assessments conducted by PHC facilities. Since the roll out of the information system in 2015, additional operational modules were added.

The system has a facility set-up section where the names of all public health facilities are populated, using the DHIS facility data, according to the following hierarchy: province, district, sub-district, facility name, facility type/classification, facility ownership and two unique identifiers. Health facilities/districts is responsible for capturing data on the web-based information system or Offline module. The system hosts web-based modules, an offline module and a mobile application developed for android and iOS operated cell phones.

The following web-based modules are available:

- Quality assessments (clinics, community health centres (CHCs) and hospitals)
- Quality Improvement Plans (QIP) (clinics, CHCs and hospitals)
- Waiting Times (clinics, CHCs)
- Facility Profile (clinics, CHCs)
- Patient Safety incident (clinics, CHCs and hospitals)
- Complaints, Compliments and Suggestions (clinics, CHCs and hospitals)

The following Offline module is available:

- Capture quality assessments, complaints/compliments/suggestions and patient safety incidents and generate a template for QIP.

The following Mobile application is available:

- Complaints App for the public to log complaints about health services provided by public health facilities.

2. Service Level Agreement

A three year service level agreement (SLA) (1 June 2021 to 31 May 2024) is signed with the system developers for hosting, maintenance, support and development of the web-based information system to ensure that there is a support, maintenance and development plan for:

- the web-based monitoring software to monitor the performance of Primary Health Care (PHC) facilities and hospitals.
- an Offline module for facilities that do not have internet connectivity. The data captured on the Offline module is exported and upload to the web-based software.
- the National Complaints APP for the public to lodge complaints about services rendered at public health facilities.

The obligations of the service provider, roles, and responsibilities of the service provider and NDoH, service level management and reporting and payment schedule is set out in the SLA.

3. System Environment

3.1 PHP

PHP version 7.3 is used.

3.2 Database connectivity

Application interface with Microsoft SQL Server via 2 Modules

- PHP Data Objects: Provides prepared and parameterised SQL statement API (Data Security)
- SQLSRV Driver: Microsoft Developed SQL Server driver for PHP

3.3 Other enabled PHP components

- Redis: in-memory database project implementing a distributed, in-memory key-value store
- PHPExcel and PHPSpreadsheet : Excel spreadsheet handling

- Swift Mailer: MIME compliant email library
- MCrypt: Encryption library, sensitive data will be encrypted with 256 bit AES encryption
- MHash: Hashing library
- MBString: Multi byte string support

3.4 Client side components

- JQuery: Javascript Library

3.5 The Framework

- Security
    - Server side validation
    - Output sanitation
    - User management and access control
    - Role and group based access control
    - Session management and security – system automatically logs out the user if the user has not been active for 30 minutes
    - Auditing (Access, Database, Actions, Performance)
- Data Handling
    - Data integration
    - Data provider abstraction
    - Filtering
    - Reporting and Charting
- Back-up infrastructure
    - Intel(R) Xeon(R) CPU E5-1620 v4 @ 3.50GHz (or latest version)
    - 32 GB RAM
    - 12 TB storage
    - VEEAM Server Intel(R) Xeon(R) CPU E5-1620 v4 @ 3.50GHz (snapshots)
    - Azure for long-term off-site back-ups
- Output Generation
    - Templating
    - Composition
    - Static resource management (CSS, Javascript and images)

4. Server Specification

A dedicated server is used for the solution. It is hosted in Xneelo’s data centre in Midrand.

4.1 Hardware

- Intel Xeon E5-1620 v4 Quad Core 3.5GHz (or latest version)
- 48GB of RAM
- 1 TB (RAID 1)
- 100 Mbit Ethernet

4.2 Network

- Upstream provided by Xneelo
- 100 Mbit bandwidth

4.3 Software

Operating System:

- Windows Server 2016 (or latest)
- Fully patched

Web Server:

- IIS 10

Database Server:

- Microsoft SQL Server 2012
- Service Pack 4 (or latest)

5. Scalability

5.1 Web Server

Currently the solution uses 1 application server (as per above specs). The system supports the scalability to add as many additional servers as deemed to be required by way of the use of a load balancer and an application server farm, with the use of Application Request Routing.

Another possible option (if & when required), will be the separation of the application server from the database server, although this would require substantially more load than expected.

5.2 Database

Microsoft SQL Server supports various technologies for scaling a solutions, such as “AlwaysOn”, clustering (replication and mirroring). These options are easy to implement, although the need is currently not expected, and there will be associated License costs.

5.3 Content

Static content could be handled by a content delivery network. Resources such as images, javascript and CSS could be handled by such a service. This is of least concern due to bandwidth availability on the server and client-side caching techniques used.

5.4 Caching

In memory cache (Redis) is used to cache database requests, opcode and files. Dedicated memcache servers can be used, if required.

5.5 Additional Security

- SSL certificate (Thawte)
- System also uses Cloudflare, a content delivery network, DDoS mitigation, Internet security solution
- SQL injection prevention

6. Users of the information system

The users of the system are staff appointed at the national and provincial departments of health and staff appointed at health directorates at local governments (applicable to Gauteng, KwaZulu-Natal and Western Cape) as well as other stakeholders where applicable.

7. Functions of the information system

7.1 Web-based modules

The system consists of the following web-based modules:

- Quality assessments (clinics, CHCs and hospitals)
    - Public health facilities conduct a self-assessment of the facility by using a quality self-assessment tool that consists of components, sub-components and elements. The elements consist of a set of measures, some of the measures have checklists attach to it to further define the measure. Clinics, CHCs and hospitals each have their own assessment tool. The results of the assessments are used to calculate

the indicators for number of Ideal Clinics, as defined in the National Indicator Data Set (NIDS) as well as to comply with Regulations (Norms and Standards Regulations applicable to different categories of health establishments (2018)) to submit an annual self-assessment report.

- Quality Improvement (clinics, CHCs and hospitals)
  - The quality improvement plan (QIP) module populates per clinic/CHC/hospital all the quality measures that were failed on their assessment. Health facilities complete the QIP form by entering a QIP (action to be taken, by whom, by when) for every failed measure. QIPs assist facilities to close the gaps identified during their quality assessments.
- Waiting Times (clinics, CHCs)
  - The Waiting time survey consist of a survey where clinics/CHCs can capture the time a patient spends in a facility. The time for each patient is captured per service area to determine the waiting time that every patient spend in the facility. Aggregate report average waiting time nationally, provincially, district and sub-district.
- Facility Profile (clinics, CHCs)
  - The profiles consist of various sections, i.e. facility contact details, social determinants of health, facility operational hours, services offered, human resources, workload and efficiency indicators, infrastructure, implementation partners and clinic committee members. It is Regulatory requirement (as set out in the Procedural Regulations pertaining to the functioning of the Office of Health Standards Compliance and Handling of Complaints by the Ombud (2016)) to submit this information to the Office of Health Standards Compliance as it is part of the submission of annual returns.
- Patient Safety Incident (PSIs) (clinics, CHCs and hospitals)
  - The Patient safety incident reporting module consists of a capture form to capture patient safety incidents that occurred at the facility. The module was developed to assist facilities to implement the National Guideline for PSI reporting and learning. The module uses the PSI data captured to calculate the three indicators for PSIs, as defined in the NIDS, i.e. PSIs cases closed, PSIs cases closed withing 60 working days and severity assessment code (SAC) 1 reported within 24 hours. The data set also provides information on the type of PSIs reported, the contributing factors and outcomes (patient and organisation) according to the World Health

    Organization's minimum information model for PSIs. The data on the classifications are used to improve the safety of care provided to patients.

- Compliments, Complaints, and Suggestions (clinics, CHCs and hospitals)
    - The Complaints, compliments and suggestion reporting module consist of a capture form for complaints, compliments and suggestions to enable facilities to capture the complaints, compliments and suggestions that they receive at the facility and other platforms. The module was developed to assist facilities to implement the National Guideline to manage Complaints, Compliments and Suggestions. The module uses the complaints data captured to calculate the two indicators, as defined in the NIDS, for complaints, i.e. complaints resolution rate and complaints resolution within 25 working days. The data set also provides data on the type of complaints captured. The data on categories of complaints is used to improve quality of services provided.

Each module except Facility Profiles and Waiting Times consists of three components: a capturing form, a reporting section and a dashboard. Facility Profiles and Waiting Time module do not have a dashboard component. The reporting components provide data per facility and aggregated reports that summarize data according to the facility level hierarchy. The dashboard components display data in graphical format. The reporting and dashboard components have various filters to enable the user to generate reports at different levels of care (national, provincial, district, sub-district, facility), ownership (provincial or local government facilities), facility type (clinic, community health centre, hospitals), period (according to the department financial years) and additional filters which is specific to each module.

7.2 Offline module

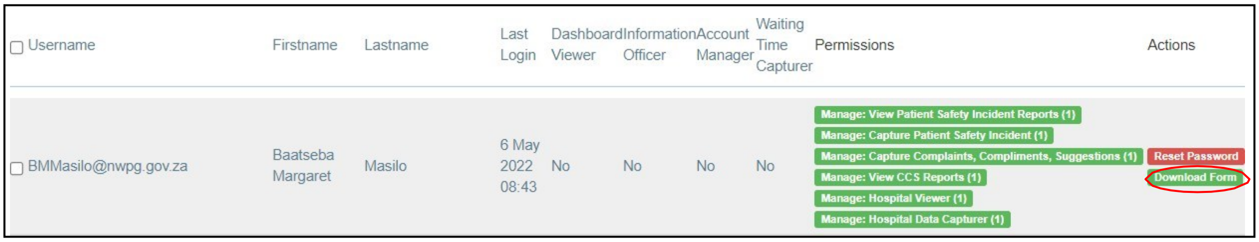
The system makes provision for an offline module for facilities to enable the facilities that do not have internet connectivity to capture data (for Clinic/CHC quality assessments, patient safety incidents and complaints, compliments and suggestion) offline by installing the offline module on a computer. The offline module has an export functionality to export a file with the data captured. The exported file is then saved on a storage device, which is usually taken to the District/Sub-district office for uploaded to the web-based information system. The offline module has limited reports to enable the facility to generate a report on the data captured.

7.3 Mobile application

A mobile application hosts the Department of Health Complaints App for the public. The App was developed to create a platform for the public to log complaints about the health services provided at public health facilities. Complaints data that is captured on the Complaints mobile App is stored in a separate database on the same database server. It is transferred to the IHF database on a daily scheduled task via a username/password authentication, so that the complaints can be processed in IHF application by the facility staff.

8. User account functionality

Access to the information system is requested by completing the Ideal Health Facility user account request form that must be digitally signed by the user as well as their supervisor, see **Annexure A**. The completed user account request forms are uploaded on the web-based information system for every account that is requested/changed or enabled, see **Figure 1**. The system checks whether all required fields have been completed before it allows upload of the form. All user account forms uploaded are saved to ensure that a history is available for all changes requested per account, therefore if multiple forms were uploaded for a specific account,all the account forms for that account are saved. The e-mail address is used as the unique identifier for the user accounts.



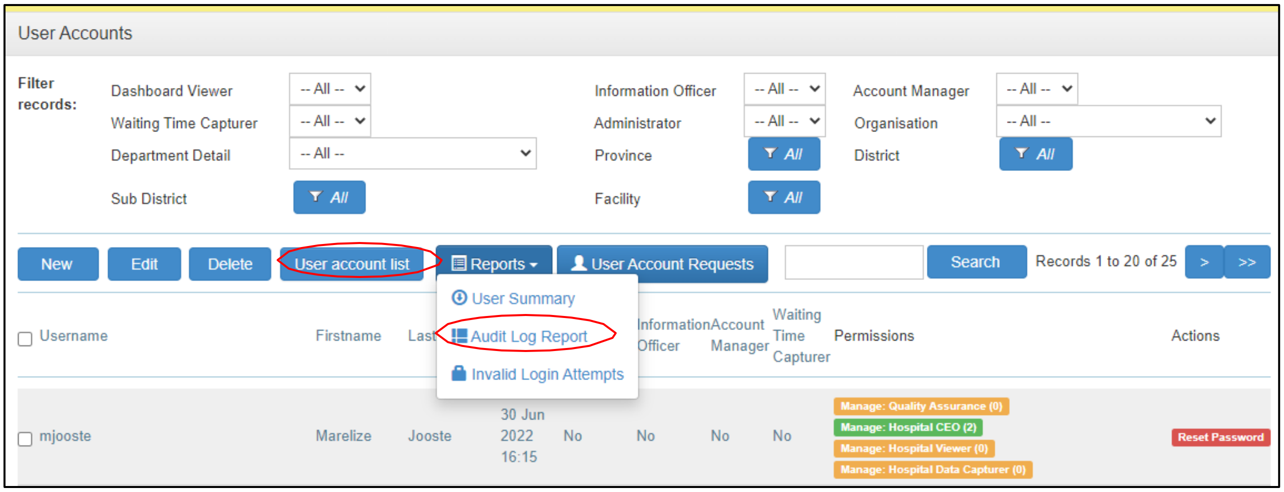
□ Username	Firstname	Lastname	Last Login	Dashboard Viewer	Information Officer	Account Manager	Waiting Time Capturer	Permissions	Actions
□ BMMasilo@nwpg.gov.za	Baatseba Margaret	Masilo	6 May 2022 08:43	No	No	No	No	Manage: View Patient Safety Incident Reports (1) Manage: Capture Patient Safety Incident (1) Manage: Capture Complaints, Compliments, Suggestions (1) Manage: View CCS Reports (1) Manage: Hospital Viewer (1) Manage: Hospital Data Capturer (1)	Reset Password Download Form

Figure 1: *Upload of user account form*

Provinces are responsible for managing their own user accounts and to set-up standardized processes for managing their user accounts. Therefore every Province issued a circular/standard operating procedure that guides staff on the procedure to request or amend user accounts.

Account managers can generate a *User Account list* that details the user accounts created for the provinces with the roles and org units assigned to every account as well as last login time, account created/terminated and whether the account is enabled (active), see **Figure 2**. The detailed procedure on how to create user accounts and generate the user account list is described in the

National SOP to manage user accounts on the Ideal Health Facility Information System. This SOP also details the requirements to review all user accounts on an annual basis.



User Accounts

Filter records:

Dashboard Viewer -- All --
Waiting Time Capturer -- All --
Department Detail -- All --
Sub District All
Information Officer -- All --
Administrator -- All --
Province All
Facility All
Account Manager -- All --
Organisation -- All --
District All

□ Username	Firstname	Last			Information Officer	Account Manager	Waiting Time Capturer	Permissions	Actions
□ mjooste	Marelize	Jooste	30 Jun 2022 16:15	No	No	No	No	Manage: Quality Assurance (0) Manage: Hospital CEO (2) Manage: Hospital Viewer (0) Manage: Hospital Data Capturer (0)	Reset Password

***Figure 2:** User account list and Audit log report*

NDoH manages accounts requested by staff working at the NDoH and other outside organisations where applicable. User account forms must also be signed electronically by the user as well their supervisor. Where outside organisations requests access, the Chief Director: District Health services must give approval for the creation of the accounts (this is only applicable for the Ideal Clinic/CHC/hospital assessments). All account requests are submitted to the National administrator for creation/amendment.

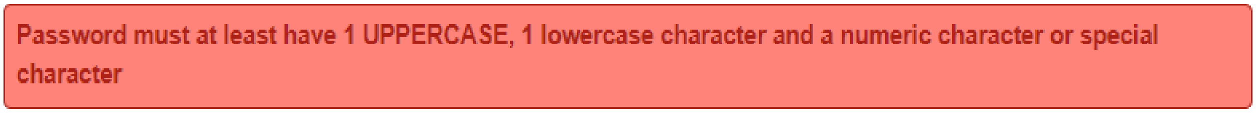
Once an account has been created, an e-mail notification is sent to the user with the username and temporary password. Once the user has logged in, the user must select their own password.

All staff that has left the service or staff that no longer require access to the information system, must complete a user account form and select the option for 'Termination' and enter the date of termination of the user account. Once a user account form is uploaded for staff that has terminated their service, the system uses the date of termination filled in on the form to insert the date of termination on the 'User Account List.'

An *Audit Log Report* is available that indicates the user who created/amended the account or who requested a password reset and the date of the amendment of the account, see **Figure 2**. The detailed procedure on how to generate the report is described in the *National SOP to manage user accounts on the Ideal Health Facility Information System.*

9. Password requirements

The password must have 8 characters, of which one is an uppercase letter, one lower case and one numerical number or special character. An error message will display if the password doesn't comply with the rule, see **Fig 3**. The system has an option where users can reset their password if they have forgotten it. This functionality is only functional if the user's account is enabled.



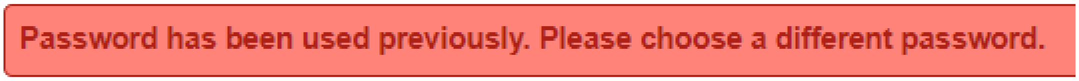
Password must at least have 1 UPPERCASE, 1 lowercase character and a numeric character or special character

Figure 3: Error message if the password doesn't comply with the rule

User accounts that have not been accessed for three consecutive months is automatically disabled. Staff must then complete a user account request form and select the option for 'Reset' password.

The Ideal Health Facility information system is a system that isn't used daily as quality assessments are conducted and captured on a quarterly (3 months) basis, therefore the password age is set at three months. Setting the password age according to leading practice (1 month) would put an additional burden on the end user who doesn't access the system every month. All users will automatically be directed to the page to reset their passwords once the three month period has been reached.

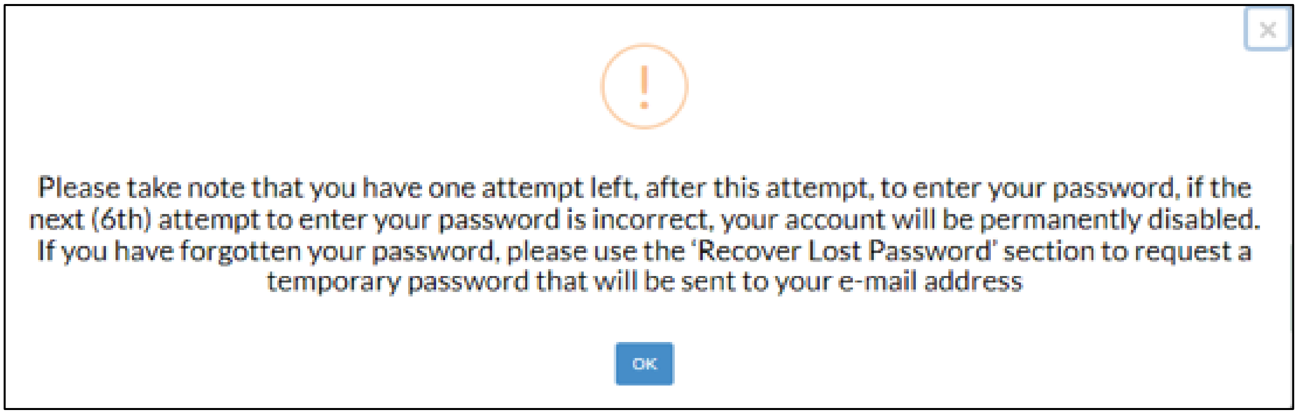
When updating passwords, the user may not use the 12 previously used passwords. An error message will display, prompting the user to select a password that was not used previously, see **Fig 4**.



Password has been used previously. Please choose a different password.

Figure 4: Error message when previous 12 passwords were used when updating passwords

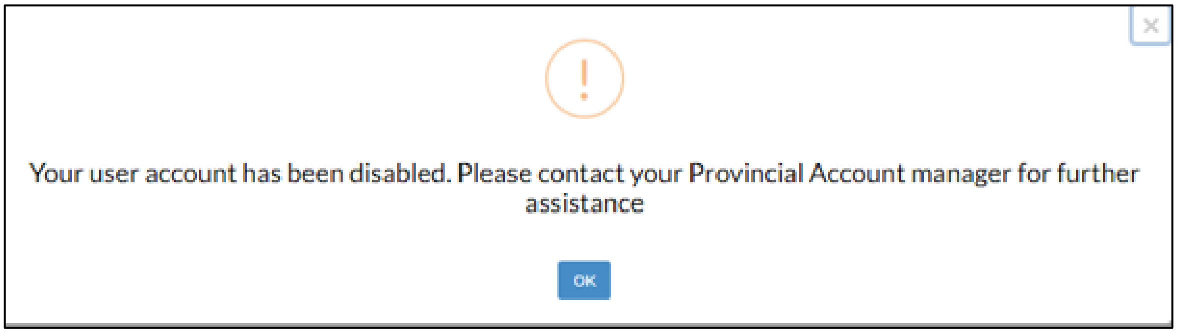
Because the end user doesn't access the system daily, the likely hood that they would forget their password is high, therefore the lock out threshold is set at six times (leading practice is three times). On the fifth (5th) incorrect password attempt a pop-up message will prompt the user that the account will be disabled on the next sixth (6th) attempt, see **Fig 5**.



Please take note that you have one attempt left, after this attempt, to enter your password, if the next (6th) attempt to enter your password is incorrect, your account will be permanently disabled. If you have forgotten your password, please use the 'Recover Lost Password' section to request a temporary password that will be sent to your e-mail address

Figure 5: Pop-up message to prompt user that account will be disabled on the sixth (6th) incorrect attempt

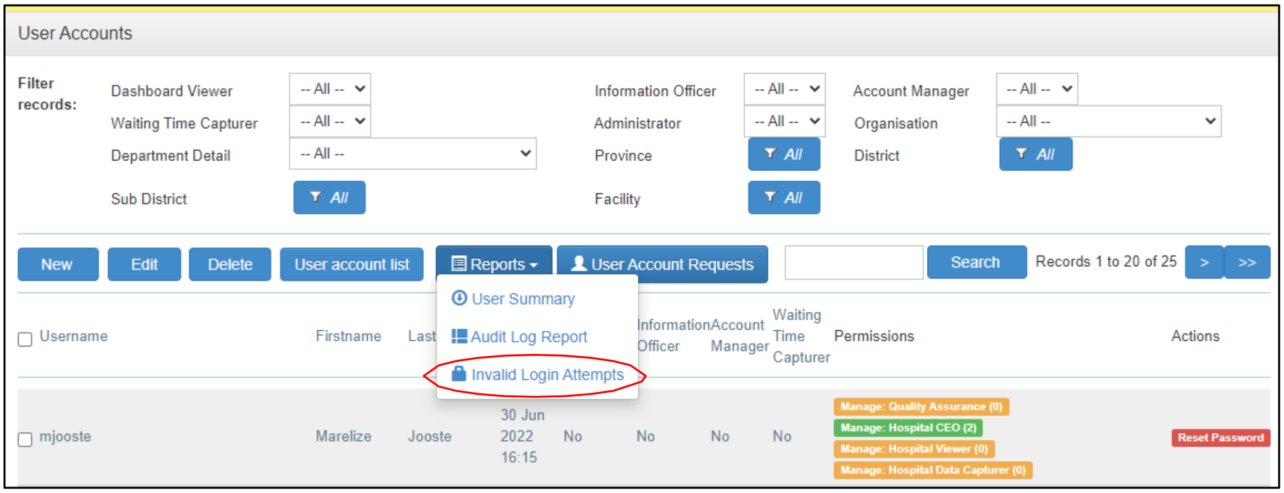
On the sixth incorrect password attempt, a pop-up message will appear to prompt the user that their account has been disabled, see **Fig 6**. The user must then complete a new user account form.



Your user account has been disabled. Please contact your Provincial Account manager for further assistance

Figure 6: Pop-up message to prompt the user that their account has been disabled after the sixth incorrect password attempt

A report is available under the *User Account* functionality to track the number of invalid login attempts, see **Figure 7** and **Figure 8**. Invalid login attempts are monitored continuously by the developers for possible hacking attempts.



User Accounts

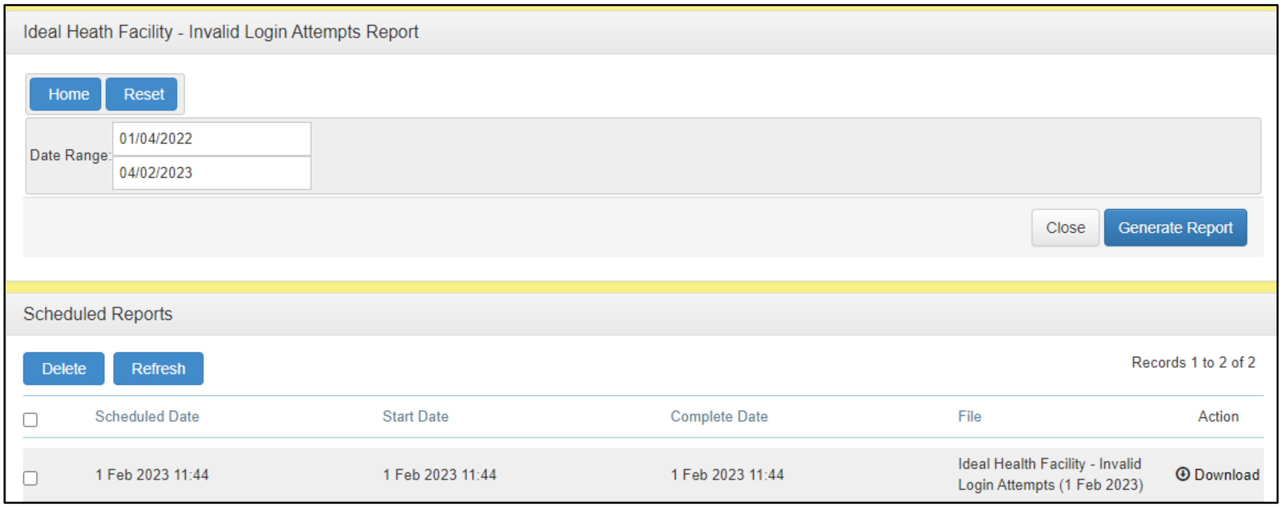
Filter records:

Dashboard Viewer	-- All --	Information Officer	-- All --	Account Manager	-- All --
Waiting Time Capturer	-- All --	Administrator	-- All --	Organisation	-- All --
Department Detail	-- All --	Province	All	District	All
Sub District	All	Facility	All		

Records 1 to 20 of 25

□ Username	Firstname	Last			Information Officer	Account Manager	Waiting Time Capturer	Permissions	Actions
□ mjooste	Marelize	Jooste	30 Jun 2022 16:15	No	No	No	No	Manage: Quality Assurance (0) Manage: Hospital CEO (2) Manage: Hospital Viewer (0) Manage: Hospital Data Capturer (0)	Reset Password

Figure 7: *Report drop-down for Invalid Login Attempts*



Ideal Heath Facility - Invalid Login Attempts Report

Date Range: 01/04/2022
04/02/2023

Scheduled Reports

Records 1 to 2 of 2

□	Scheduled Date	Start Date	Complete Date	File	Action
□	1 Feb 2023 11:44	1 Feb 2023 11:44	1 Feb 2023 11:44	Ideal Health Facility - Invalid Login Attempts (1 Feb 2023)	Download

Figure 8: Generate Invalid Login Attempts report

10. Roles and permissions for user accounts

There are seven types of roles that can be assigned to an account. See **Table 1** that describes the functions of the roles.

Type of roles	**Function of roles allows the user to:**
View	• View the reporting and dashboard section
Capture	• Capture data
Authorise	• Applicable for hospital module where there is a role to authorize as Quality Assurance manager of Chief Executive Officer.
Data Controller (Administrator)	• Re-open closed/resolved PSIs and Complaint forms • Delete PSI and CCS forms.
Notifications contact manager	• Enable the user to set-up notifications for staff to receive an e-mail or SMS when a Severity Assessment Code one PSI was logged on the system.
Account Manager	• Create and amend user accounts
Administrator	• Development, maintenance and security of the system

Table 1: Roles and functions of user accounts

Permissions are assigned for each role according to the specific level (facility, district, sub-district, provincial) requested on the user account form. Permission level can also be assigned according to the ‘ownership’ of the facilities, this only apply to user accounts created for Gauteng, KwaZulu-Natal and Western Cape that have facilities that is ‘owned’ by local government.

11. NDoH service desk support to the end user

Service desk support is provided at idealclinic@health.gov.za. Once a request for support is submitted by the end user (provincial/district/facility staff), the request is logged by the NDoH project manager on the *Jira Service Management* application (https:// asgsolutions. atlassian.net/ servicedesk /customer/portals) which it the service desk application that is used to manage service desk requests.

The subject line for all the end-user support cases is recorded as *NDoH Helpdesk*, followed by the name of the province/district/facility who sent the request for support and a short description of the support requested. This is to ensure that cases logged for end user support and cases logged to the service provider (developer) for support or change requests (development) can be distinguished from each other. Once a case for end user support is logged, a service desk case number is assigned. The NDoH project manager responds via e-mail to the end user with updates on the case and the reference number for the case is indicated in the subject line of the e-mail. All communication sent via e-mail is logged on the service desk case. Once the case has been resolved the end user is informed via e-mail and the case is closed on Jira. Each case is assigned with a priority, the priority levels are described in **Table 2**.

Table 2: Priority levels for NDoH service desk support

Priority	**Description of priority level**	**Turn around time for priority level**
Blocker	An issue that affects the use of the software across the installation base of the application(s). The application is completely down or inoperable.	4 hours
Critical	An issue with a known work around, affects a single or group of user/s and is critical to be addressed as soon as possible.	8 hours (1 working day). If a full resolution is not possible within the 8 hours, the NDoH will strive to provide a temporary work-around where possible and will communicate with the end user on progress made.
Major	An issue with a known work around, affects a single or group of user/s and is not critical to be addressed immediately.	16 hours (2 working days) If a full resolution is not possible within the 16 hours, the NDoH will strive to provide a temporary work-around where possible and will communicate with the end user on progress made.
Minor	A change request/enhancement/issue that does not need immediate attention but is important to improve the client's experience.	32 hours (4 working days). If a full resolution is not possible within the 32 hours, the NDoH will strive to provide a temporary work-around where possible and will communicate with the end user on progress made.

12. System support and change requests from NDoH to service provider (developers)

System support and change requests for development of the information system to the developer (service provider) are logged on the service desk. The service desk application that is used, is the *Jira Service Management* application (https://asgsolutions.atlassian.net/servicedesk/). The Project manager of NDoH logs all requests for support and change requests for development on the service desk.

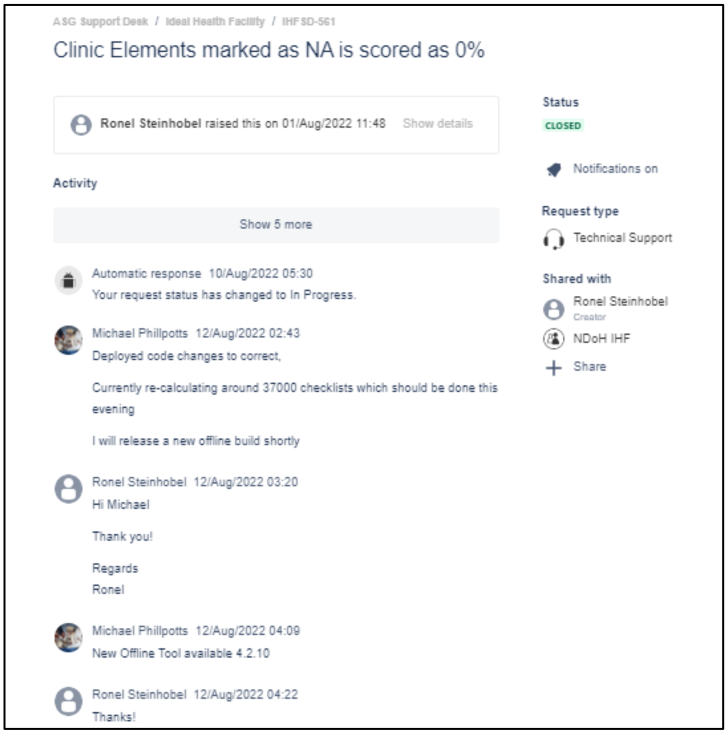
12.1 Change request documentation

Once a request has been logged, a service desk case number is assigned for the service desk request and the priority level is assigned (**Table 3)**.

Table 3: Priority levels for Service provider service desk support

Priority	Description of priority level	Turn around time for priority level
Blocker	An issue that affects the use of the software across the installation base of the application(s). The application is completely down or inoperable.	4 hours
Critical	An issue with a known work around, affects a single or group of user/s and is critical to be addressed as soon as possible.	8 hours (1 working day). If a full resolution is not possible within the 8 hours, the service provider will strive to provide a temporary work-around and will agree with the NDoH on a reasonable time for full resolution and continuously provide updates on the progress made.
Major	An issue with a known work around, affects a single or group of user/s and is not critical to be addressed immediately.	16 hours (2 working days) If a full resolution is not possible within the 16 hours, the service provider will strive to provide a temporary work-around and will agree with the NDoH on a reasonable time for full resolution and continuously provide updates on the progress made.
Minor	A change request/enhancement/issue that does not need immediate attention but is important to improve the client's experience.	32 hours (4 working days). If a full resolution is not possible within the 16 hours, the service provider will strive to provide a temporary work-around and will agree with the NDoH on a reasonable time for full resolution and continuously provide updates on the progress made. Because change requests can be infinitely large, every effort will be made to address small changes in a timely manner.

All changes identified within the service desk case are captured with an Issue Key number to ensure that all change requests made within the service desk request are addressed. See **Fig 9** as an example of a service desk request. The service desk case documentation serves as the change request documentation as it captures all communication between the NDoH and the service provider.



ASG Support Desk / Ideal Health Facility / IHFSD-561

Clinic Elements marked as NA is scored as 0%

Ronel Steinhobel raised this on 01/Aug/2022 11:48 Show details

Activity

Show 5 more

Automatic response 10/Aug/2022 05:30
Your request status has changed to In Progress.

Michael Phillpotts 12/Aug/2022 02:43
Deployed code changes to correct.

Currently re-calculating around 37000 checklists which should be done this evening

I will release a new offline build shortly

Ronel Steinhobel 12/Aug/2022 03:20
Hi Michael

Thank you!

Regards
Ronel

Michael Phillpotts 12/Aug/2022 04:09
New Offline Tool available 4.2.10

Ronel Steinhobel 12/Aug/2022 04:22
Thanks!

Status: CLOSED

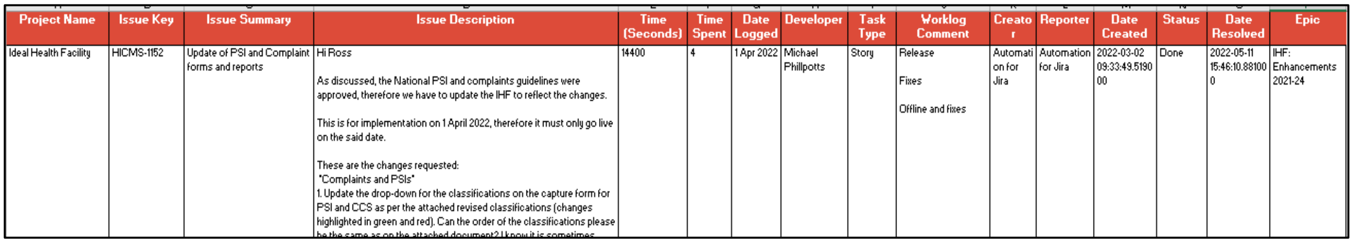
Notifications on

Request type: Technical Support

Shared with: Ronel Steinhobel (Creator), NDoH IHF

Figure 9: Screenshot of support desk

A worklog of all cases logged and status of each case can be generated from Jira, see **Figure 10** as an example. Change requests are first published on the test site (https://test.idealhealthfacility.org.za/) for review by NDoH before it is published on the live/production site. Once published on the production site, it is reviewed by NDoH and the case is closed once NDoH indicates that the development is functional.



Project Name	Issue Key	Issue Summary	Issue Description	Time (Seconds)	Time Spent	Date Logged	Developer	Task Type	Worklog Comment	Creato r	Reporter	Date Created	Status	Date Resolved	Epic
Ideal Health Facility	HICMS-1152	Update of PSI and Complaint forms and reports	Hi Ross As discussed, the National PSI and complaints guidelines were approved, therefore we have to update the IHF to reflect the changes. This is for implementation on 1 April 2022, therefore it must only go live on the said date. These are the changes requested: "Complaints and PSIs" 1. Update the drop-down for the classifications on the capture form for PSI and CCS as per the attached revised classifications (changes highlighted in green and red). Can the order of the classifications please be the same as on the attached document? I know it is sometimes	14400	4	1 Apr 2022	Michael Phillpotts	Story	Release Fixes Offline and fixes	Automati on for Jira	Automation for Jira	2022-03-02 09:33:49.5190 00	Done	2022-05-11 15:46:10.88100 0	IHF: Enhancements 2021-24

Figure 10: Example of a worklog

12.2 Service desk case management report for change requests for development

A report is compiled for every service desk request that is logged for development before the development is executed. The impact assessment forms part of the report. The NDoH project manager drafts the section for the reason for the change request as well as the description of the changes/development requested. The project manager of the service provider then documents the remainder of the sections. The service desk case management report contains the following information:

- Service desk case number
- Project manager
- Date complied/updated
- Estimated date of implementation
- Issue Keys related to the service desk case (where applicable)
- Reason for making the change request
- Description of the change request
- System structures that will be impacted by the change request
- Risk identified for implementing the change request
- Mitigation action if change is not successful when moved from UAT to production
- Estimation development cost

12.3 Approval process for change and support requests

The *Jira Service Management* application used for the service desk requests captures all communication between the NDoH and the service provider, indicating the date, time and person who captured the request/change. It is the responsibility of the NDoH project manager to log all support and development requests on the service desk. The project manager of the service provider oversees the implementation and coordination of the requests and assigns the cases to a specific developer or in some cases, more than one developer. The project manager of the service provider and the assigned developer/s is responsible to respond on communication logged by the NDoH project manager on the service desk. The service desk case documentation serves as the documentation for granting the developers approval to execute requests for support and development, including moving developments from the test instance to the production site and for closing of cases once it has been deployed on the production site.

12.4 Testing of changes

All development changes are developed on the test site. Once the development on the test site is completed, the developer logs an entry on the service desk application indicating that the development has been completed and is ready for testing. The NDoH project manager will then test the new development on the test site. If the development is according to the specifications, the project manager grants approval for the developers to take the development to the production site by making an entry on the service desk, indicating that the development can be taken to the production site.

12.5 Migration of changes to production

Once the development is on the production site, the developer logs an entry on the service desk application indicating that the development is available on the production site for review. The NDoH project manager will then review the new development on the production site. If the development is functional, the NDoH project manager grants approval for the developers to close the case on the service desk.

13. Training

The NDoH hosted provincial workshops in 2015 when the Ideal Clinic Realisation and Maintenance programme was rolled roll-out to provinces. Staff were trained during the workshops to capture data and to generate reports from the information system. When the user account functionality was handed over to provinces (2019 to 2020), additional training was conducted for provincial and district account managers to manage user accounts.

The responsibility for training of newly appointed staff is the responsibility of Provincial Departments of Health. In-service training by staff who have already been training must be conducted for newly appointed staff. A register of the in-service training of newly appointed staff must be kept as evidence of training conducted.

Training guides are available to assist staff to capture data and generate reports and dashboards. The training guides can be downloaded under the ‘Data management’ tab of the website.

A test site is also available at https://test.idealhealthfacility.org.za/ that is used to train staff.

14. Back-up procedure and Disaster recovery plan

The back-up procedure is as follows:

SQL Transactional Backup:

- The SQL database will be backed up every 15 minutes to ensure minimal data loss in case of any disaster.
- The transactional backup will be stored on a designated local storage.

Onsite Full Backup:

- A full backup of all data will be performed every day and stored on a designated local storage.
- The onsite full backup will be automatically run daily.

Offsite Full Backup:

A full backup of all data will be performed every day and transferred securely using SFTP to an offsite location.

- The offsite full backup will be automatically run daily.
- The offsite backup will be stored for 30 days to meet the requirement for data retention.
- Access to the offsite backup will be restricted to authorized personnel only.

Offsite Full Cloud Backup:

- A monthly full backup of all data is transferred securely to an Azure Blob Storage account (South Africa North)
- The backup will be stored for 13 months.
- Access to the offsite backup will be restricted to authorized personnel only.

The disaster recovery plan (DRP) and the testing thereof are described in the DRP standard operating procedure.

15. Intellectual Property

Intellectual property is the sole and exclusive property of the NDoH. Foreground Intellectual Property (e.g. M&E data collection templates and resultant data interpretations) also belongs to the NDoH. Background Intellectual property contained in the Service Provider's source code will remain the property of the Service Provider, with NDoH having rights to use this intellectual property for as long as Maintenance fees are paid. Should the NDoH exercise its right not to renew the service level agreement at the end of term, the Service Provider will provide the NDoH with the latest copy of the source code and associated data base(s) for its own use. The Service

Provider will provide no further warrantee for the software thereafter.

16. Confidentiality of data

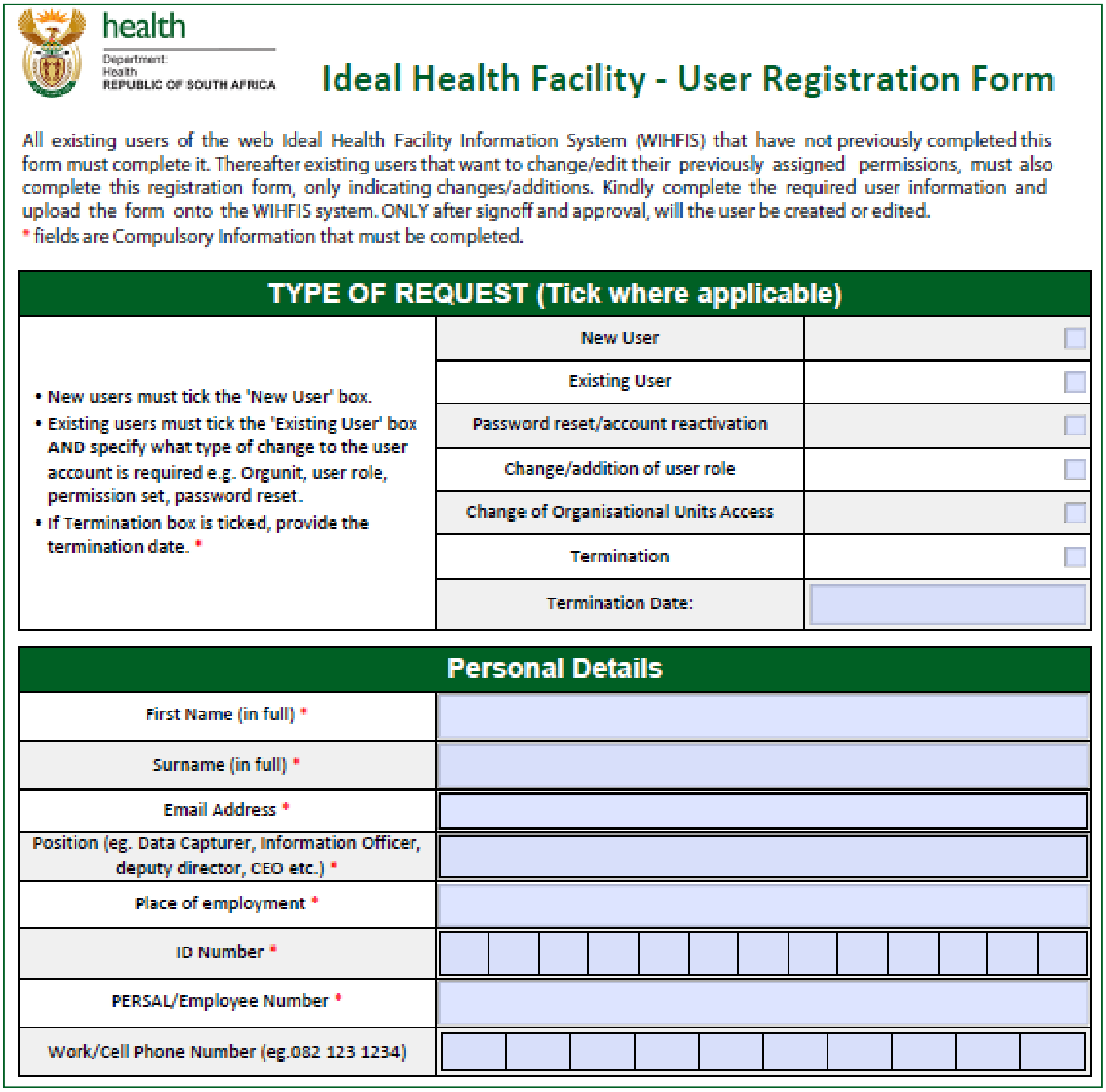
Data containing patient information will not be published in accordance with the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000) (PAIA) and the Protection of Personal Information Act, 2013 (Act 4 of 2013). PAIA gives effect to the constitutional right of access to any information held by the state and any information held by any other person, provided that such information is required for the exercise or protection of any rights. The Protection of Personal Information give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at:

(i) balancing the right to privacy against other rights, particularly the right of access to information; and

(ii) protecting important interests, including the free flow of information within the Republic and across international borders.

It is only the PSI and Complaints, compliments and suggestion modules that contains patient information. The fields for name and surname of patient in the PSI module are not mandatory fields as anonymizing the data is encouraged. The field for patient file is compulsory to complete and is used and the patient identifier.

Annexure A: Ideal Health Facility - User Registration Form



health
Department:
Health
REPUBLIC OF SOUTH AFRICA

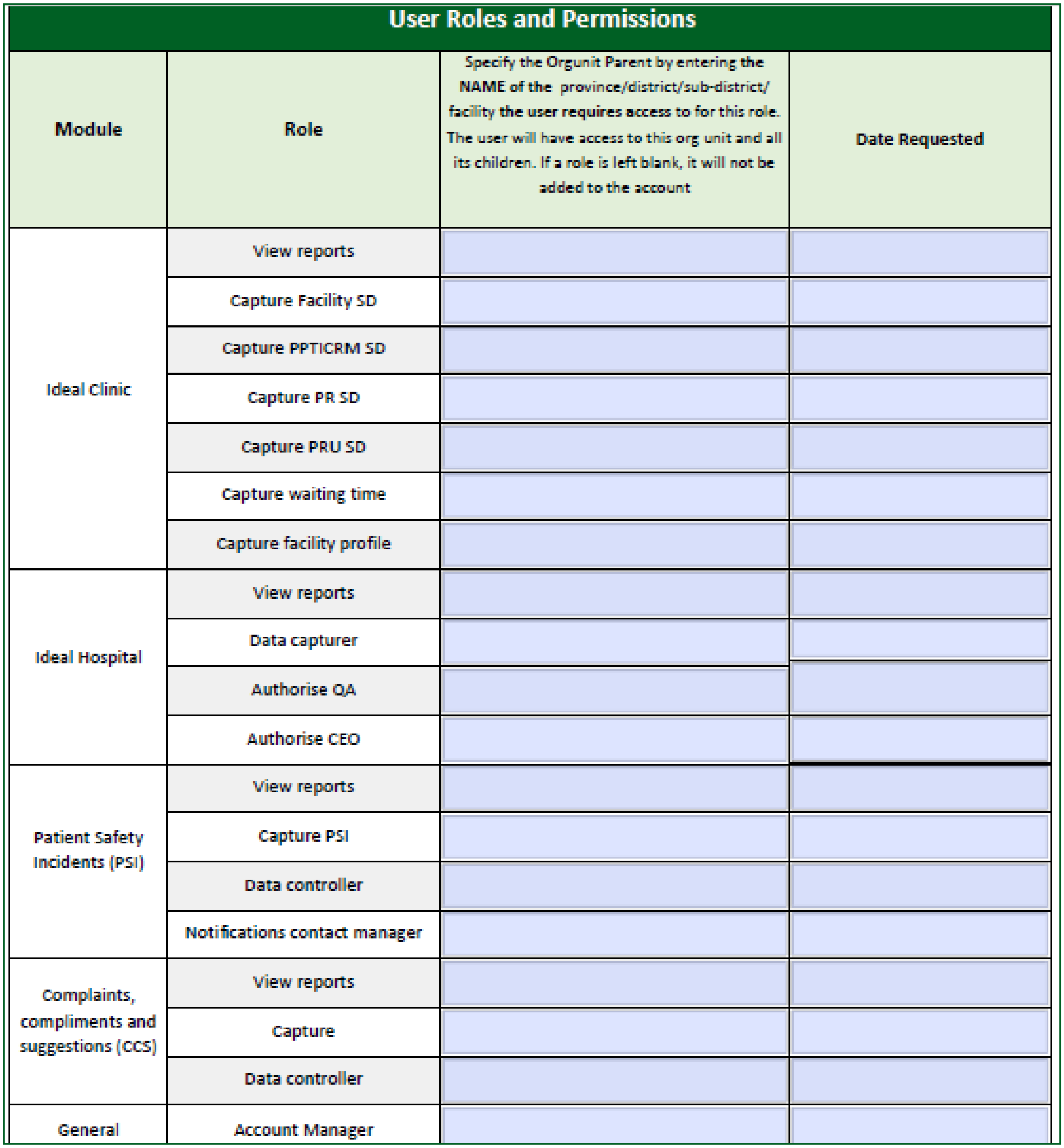
Ideal Health Facility - User Registration Form

All existing users of the web Ideal Health Facility Information System (WIHFIS) that have not previously completed this form must complete it. Thereafter existing users that want to change/edit their previously assigned permissions, must also complete this registration form, only indicating changes/additions. Kindly complete the required user information and upload the form onto the WIHFIS system. ONLY after signoff and approval, will the user be created or edited.

* fields are Compulsory Information that must be completed.

TYPE OF REQUEST (Tick where applicable)		
- New users must tick the 'New User' box. - Existing users must tick the 'Existing User' box AND specify what type of change to the user account is required e.g. Orgunit, user role, permission set, password reset. - If Termination box is ticked, provide the termination date. *	New User	□
	Existing User	□
	Password reset/account reactivation	□
	Change/addition of user role	□
	Change of Organisational Units Access	□
	Termination	□
	Termination Date:	

Personal Details	
First Name (in full) *	
Surname (in full) *	
Email Address *	
Position (eg. Data Capturer, Information Officer, deputy director, CEO etc.) *	
Place of employment *	
ID Number *	□□□□□□□□□□□□□
PERSAL/Employee Number *	
Work/Cell Phone Number (eg.082 123 1234)	□□□□□□□□□□



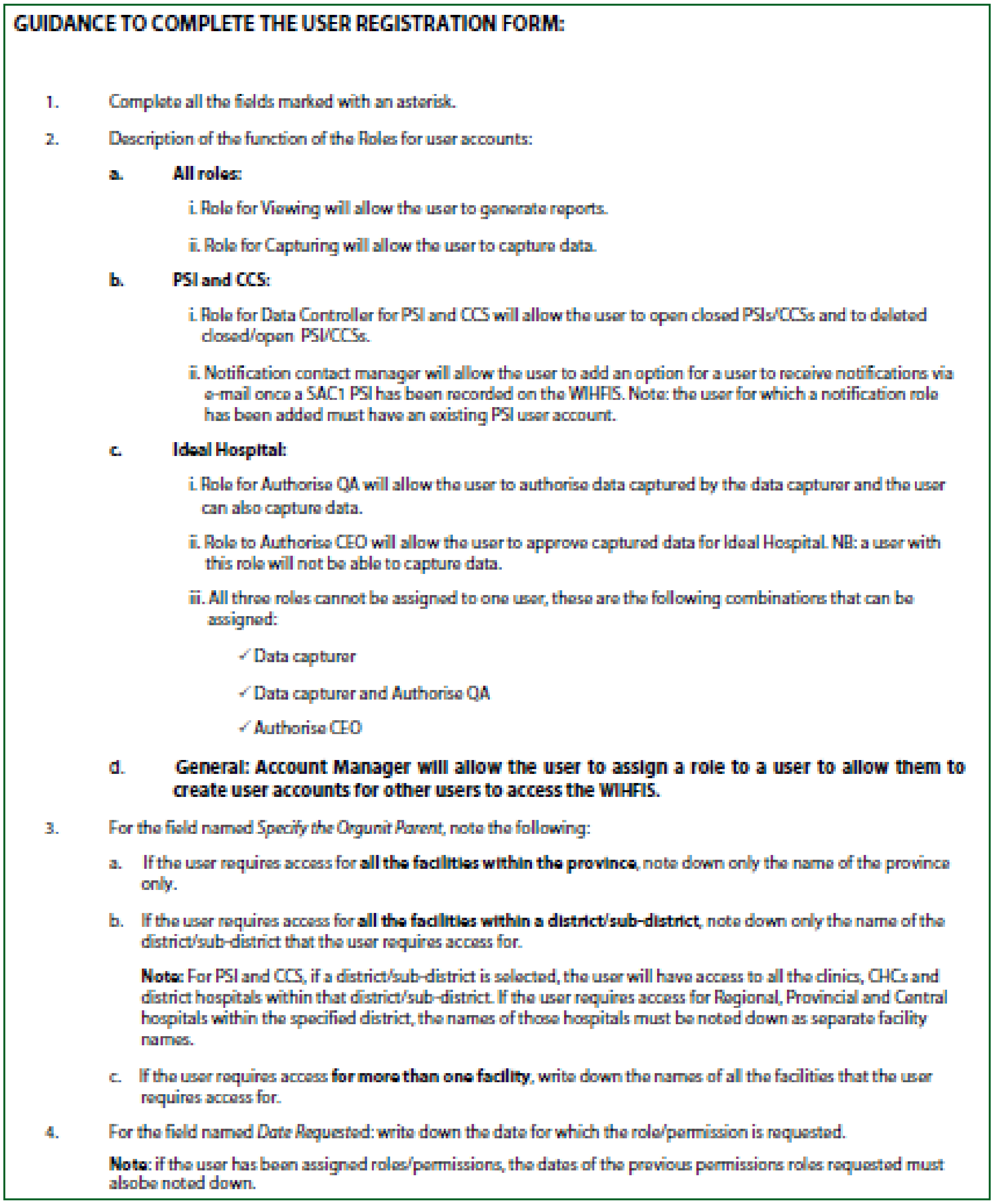
User Roles and Permissions

Module	Role	Specify the Orgunit Parent by entering the NAME of the province/district/sub-district/ facility the user requires access to for this role. The user will have access to this org unit and all its children. If a role is left blank, it will not be added to the account	Date Requested
Ideal Clinic	View reports		
	Capture Facility SD		
	Capture PPTICRM SD		
	Capture PR SD		
	Capture PRU SD		
	Capture waiting time		
	Capture facility profile		
Ideal Hospital	View reports		
	Data capturer		
	Authorise QA		
	Authorise CEO		
Patient Safety Incidents (PSI)	View reports		
	Capture PSI		
	Data controller		
	Notifications contact manager		
Complaints, compliments and suggestions (CCS)	View reports		
	Capture		
	Data controller		
General	Account Manager		

Authorisation

User's authorisation			
Date of user's signature *		User's signature *	
Manager's authorisation			
Manager's name *		Manager's surname *	
Manager's position *		Manager's contact number	□□□□□□□□□□
Date of manager's signature *		Manager's signature *	

* is required fields



GUIDANCE TO COMPLETE THE USER REGISTRATION FORM:

1. Complete all the fields marked with an asterisk.
2. Description of the function of the Roles for user accounts:

   a. **All roles:**

   i. Role for Viewing will allow the user to generate reports.

   ii. Role for Capturing will allow the user to capture data.

   b. **PSI and CCS:**

   i. Role for Data Controller for PSI and CCS will allow the user to open closed PSIs/CCSs and to deleted closed/open PSI/CCSs.

   ii. Notification contact manager will allow the user to add an option for a user to receive notifications via e-mail once a SAC1 PSI has been recorded on the WIHFIS. Note: the user for which a notification role has been added must have an existing PSI user account.

   c. **Ideal Hospital:**

   i. Role for Authorise QA will allow the user to authorise data captured by the data capturer and the user can also capture data.

   ii. Role to Authorise CEO will allow the user to approve captured data for Ideal Hospital. NB: a user with this role will not be able to capture data.

   iii. All three roles cannot be assigned to one user, these are the following combinations that can be assigned:

   ✓ Data capturer

   ✓ Data capturer and Authorise QA

   ✓ Authorise CEO

   d. **General: Account Manager will allow the user to assign a role to a user to allow them to create user accounts for other users to access the WIHFIS.**

3. For the field named *Specify the Orgunit Parent*, note the following:

   a. If the user requires access for **all the facilities within the province**, note down only the name of the province only.

   b. If the user requires access for **all the facilities within a district/sub-district**, note down only the name of the district/sub-district that the user requires access for.

   Note: For PSI and CCS, if a district/sub-district is selected, the user will have access to all the clinics, CHCs and district hospitals within that district/sub-district. If the user requires access for Regional, Provincial and Central hospitals within the specified district, the names of those hospitals must be noted down as separate facility names.

   c. If the user requires access **for more than one facility**, write down the names of all the facilities that the user requires access for.

4. For the field named *Date Requested*: write down the date for which the role/permission is requested.

   Note: if the user has been assigned roles/permissions, the dates of the previous permissions roles requested must alsobe noted down.