No.

JAPAN INTERNATIONAL COOPERATION AGENCY (JICA)
MINISTRY OF HEALTH, ISLAMIC REPUBLIC OF PAKISTAN

THE STUDY ON IMPROVEMENT OF MANAGEMENT INFORMATION SYSTEMS IN HEALTH SECTOR IN THE ISLAMIC REPUBLIC OF PAKISTAN

DHIS SOFTWARE MANUAL

FEBRUARY 2007

NATIONAL HEALTH INFORMATION RESOURCE CENTER
SYSTEM SCIENCE CONSULTANTS INC.

H M
J R
0 6 - 4 6

Japan International Cooperation Agency
Ministry of Health, Islamic Republic of Pakistan

THE STUDY ON IMPROVEMENT OF MANAGEMENT INFORMATION SYSTEMS IN HEALTH SECTOR IN THE ISLAMIC REPUBLIC OF PAKISTAN

FINAL REPORT

DHIS SOFTWARE MANUAL

February 2007

System Science Consultants Inc

PART I

QUICK START USER MANUAL

District Health Information System

Sub Contracted Work on Computer System Development

for the Study on

Improvement of Management Information System in Health Sector in The Islamic Republic of Pakistan

Quick Start User Manual

Category	Information
Customer	System Science Consultants Inc.
Project	Development of District Health Information System
Document	Quick Start User Manual
Document Version	1.0
Document Status	Final
Identifier	SSC/QSUserManual/1.0
Author(s)	AZM Project Management Team
Approver(s)	SSC
Issue Date	20th February, 2007
Last Revision	
Distribution	1. AZM 2. SSC

Contents at a glance

Sr #	Chapter	Page #
1	Log in to DHIS Application	3
	Log in	4
	Main Interface	5
2	User Management	6
	Create New User	7
	User Rights	9
	Change Password	11
3	Data Entry (Monthly Reports)	12
	New Monthly Report	13
	Edit Existing Monthly Report	16
4	Reports	19
	Monthly Reports	20
	Aggregated Reports	20
	Indicator Based Reports	22
	Printing Options	22
5	Data Management (Upward Synchronization)	23
	Create Batch file (Entered Data)	24
	Restore Form (New Forms)	24
	Data Management (Downward Synchronization)	25
	Restore Saved data	25
	Create Batch file (New Forms)	25
	Backup Database	26
	Restore Data	26
	Export Data to Excel	27

Log in Screen

Activities	Steps Involved	Action	Figure
Log in to DHIS	Type the web address in Explorer to login for your DHIS application ***http://localhost:81/DHIS***	Type User name and password then press Submit button to login to DHIS Application	Figure 1
Main Interface Screen	Interface showing your Province picture	Menu bar showing the different options for working, Province background, Data/Time and	Figure 2

Login in to DHIS

To login in the DHIS software follow the instruction provided here;

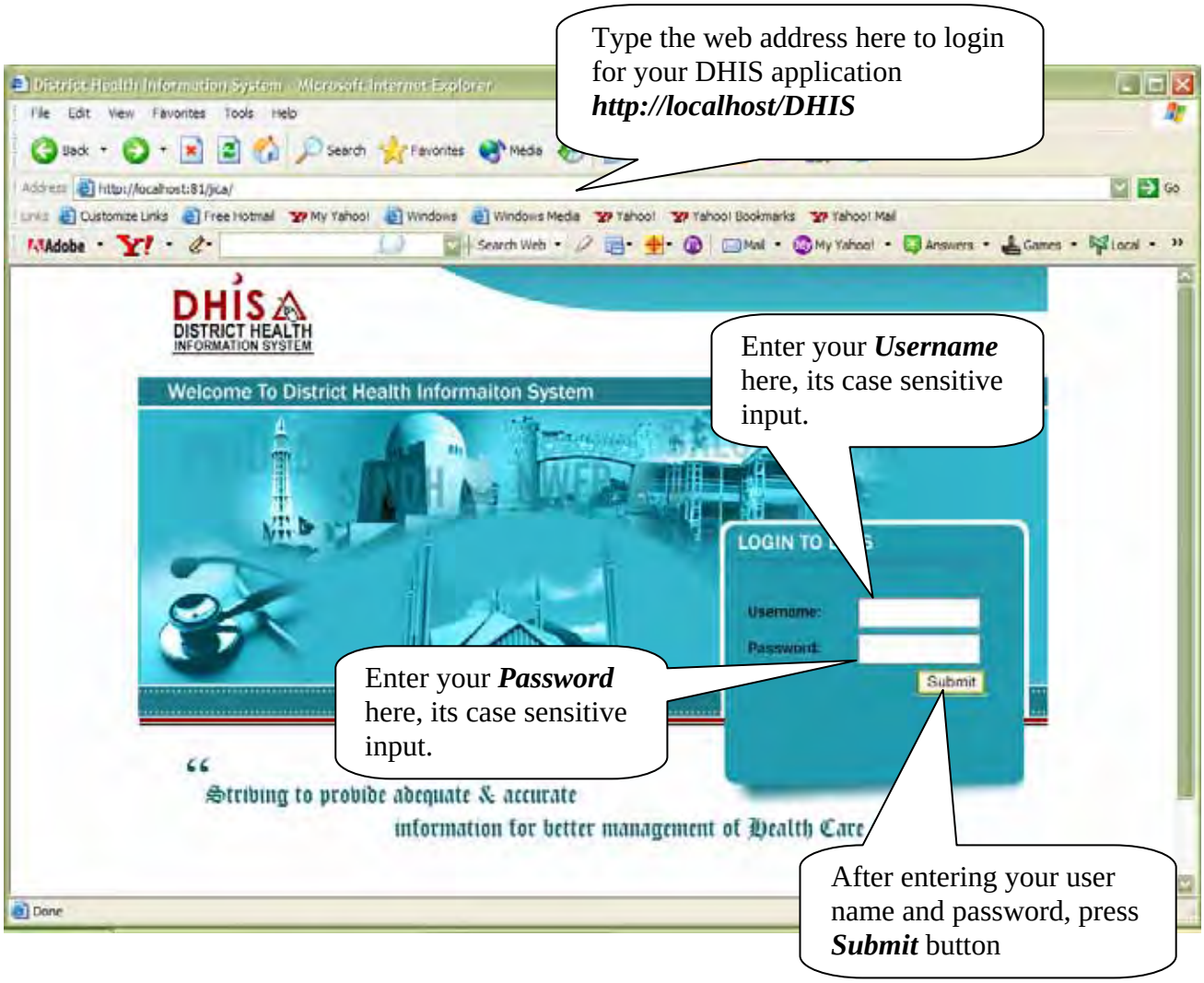


Figure 1

Main Interface/Screen

After long in, following screen will appear in your web browser; right hand side showing the picture of your province and the left hand side with menu for your selection.

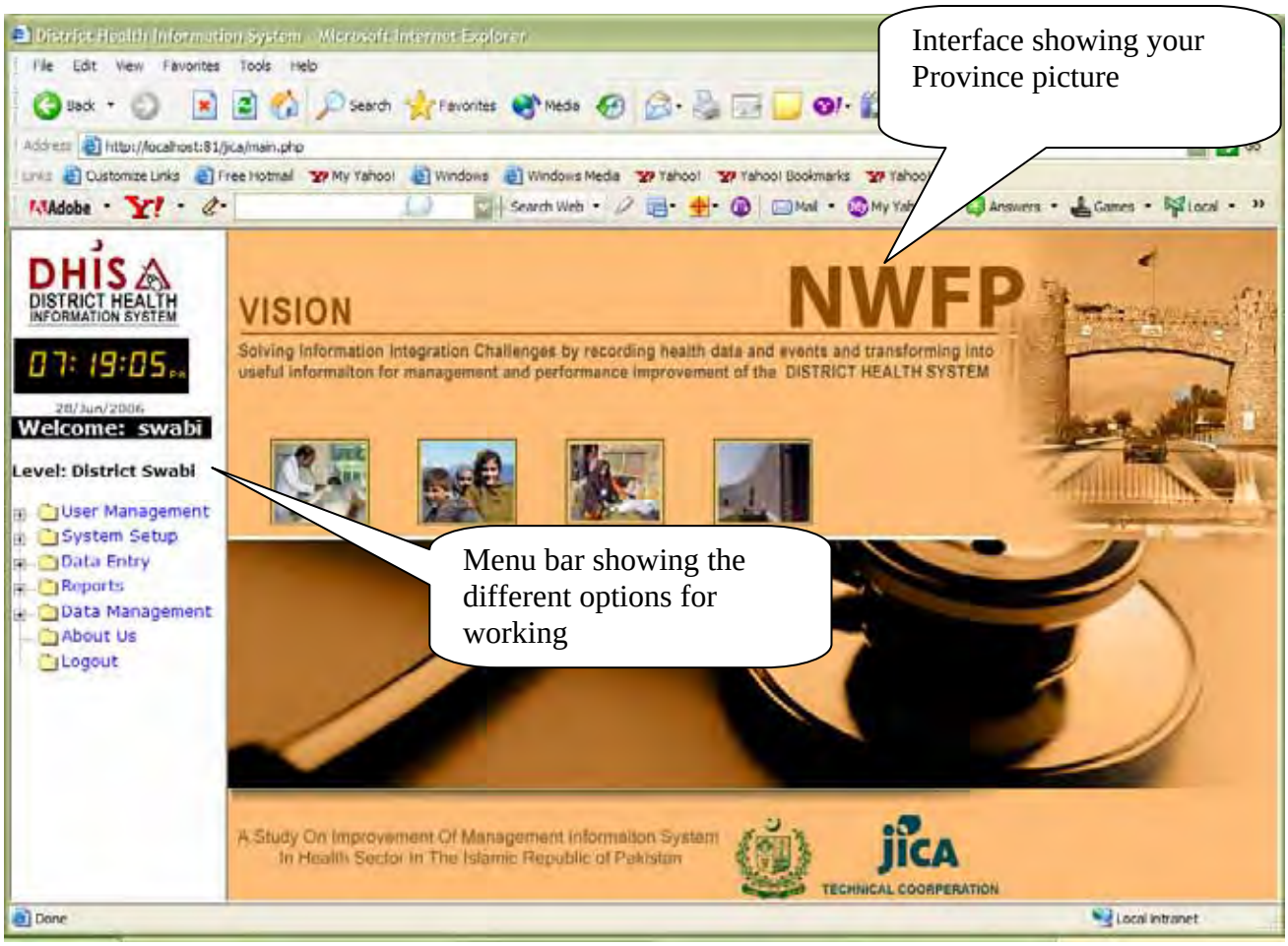


Figure 2

User Management

Activities	Steps Involved	Action	Figure
User Management	Click on the + sign against the User	To call screen; click on ***Users Accounts***	Figure 3,4
Crate New User	User Management → ***Create a New User***	Provide information for user and press Save button	Figure 5,6
User Rights	User Management → ***User Rights***	Click on ***Button*** to call the rights assignment screen	Figure 7,8,9
Change Password	User Management → ***Change password***	Enter the password information and press save button	Figure 10,11

Add New User

To add new user in the DHIS software, follow the following instructions;

1. Select User Management Option from the left side menu

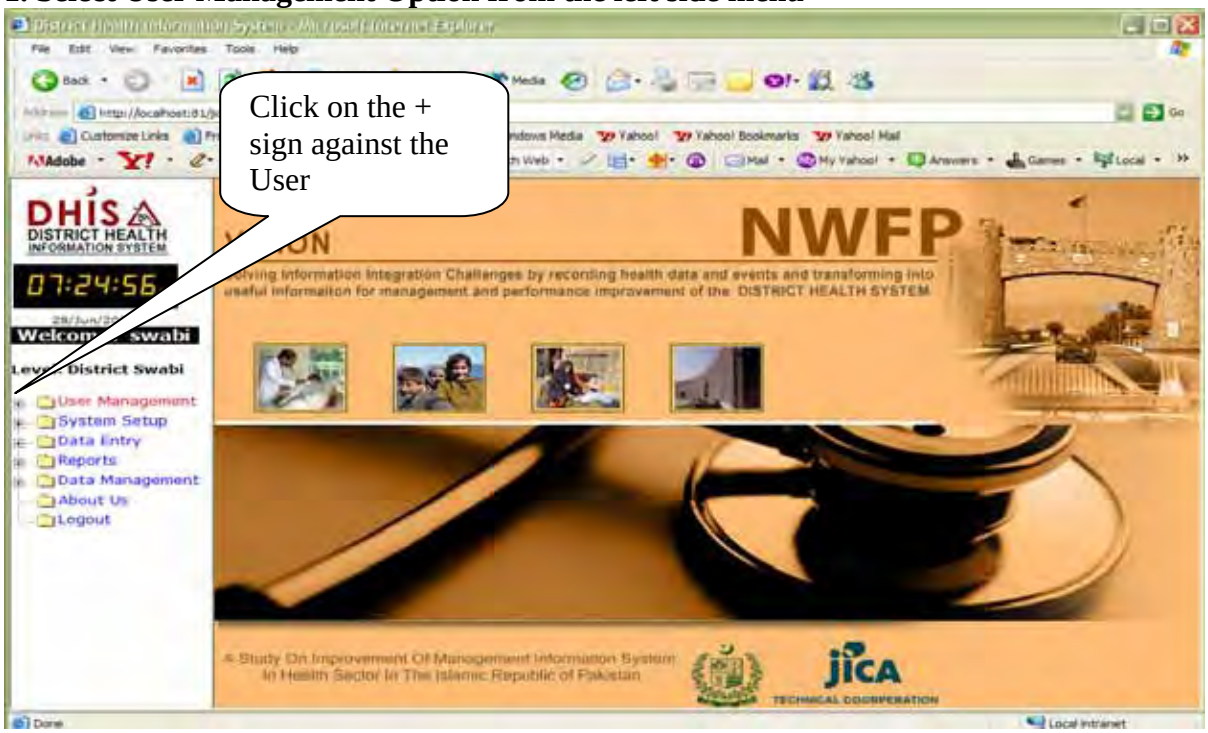


Figure 3

2. Select User Accounts Option from the left side menu

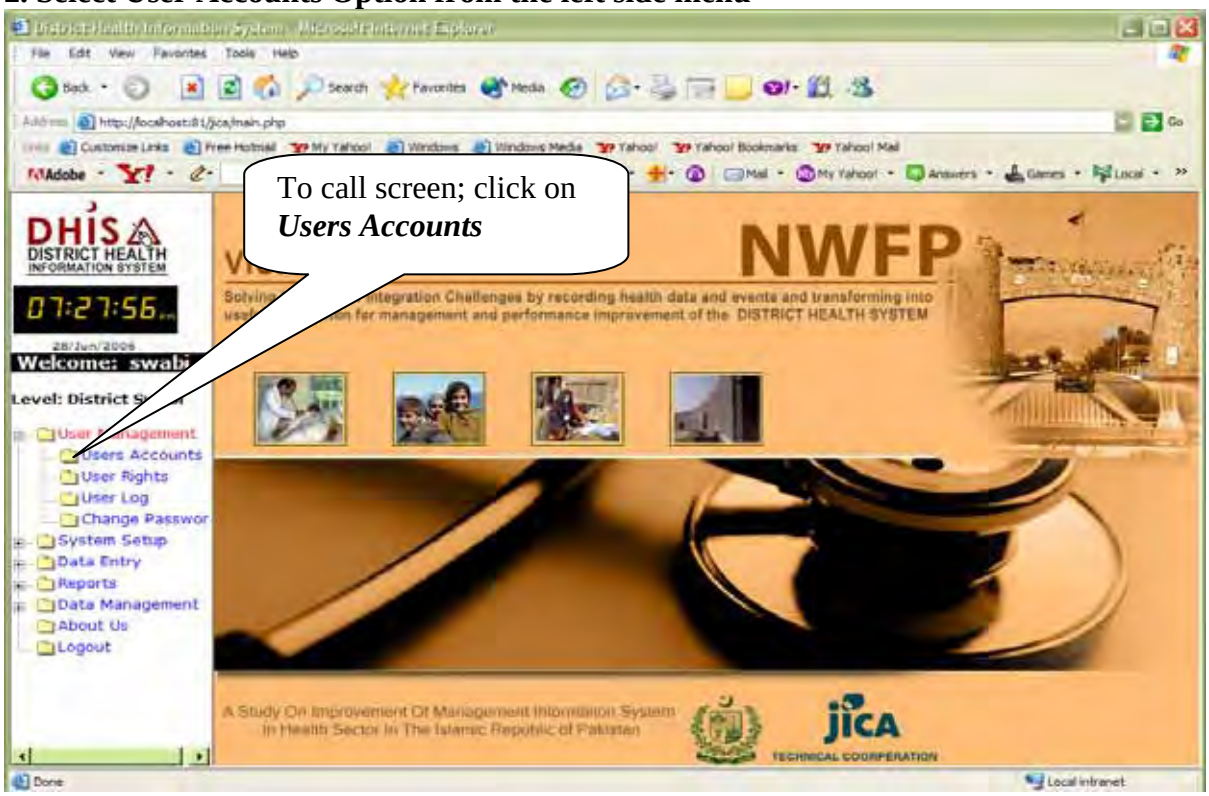


Figure 4

Click on Create a New User Account

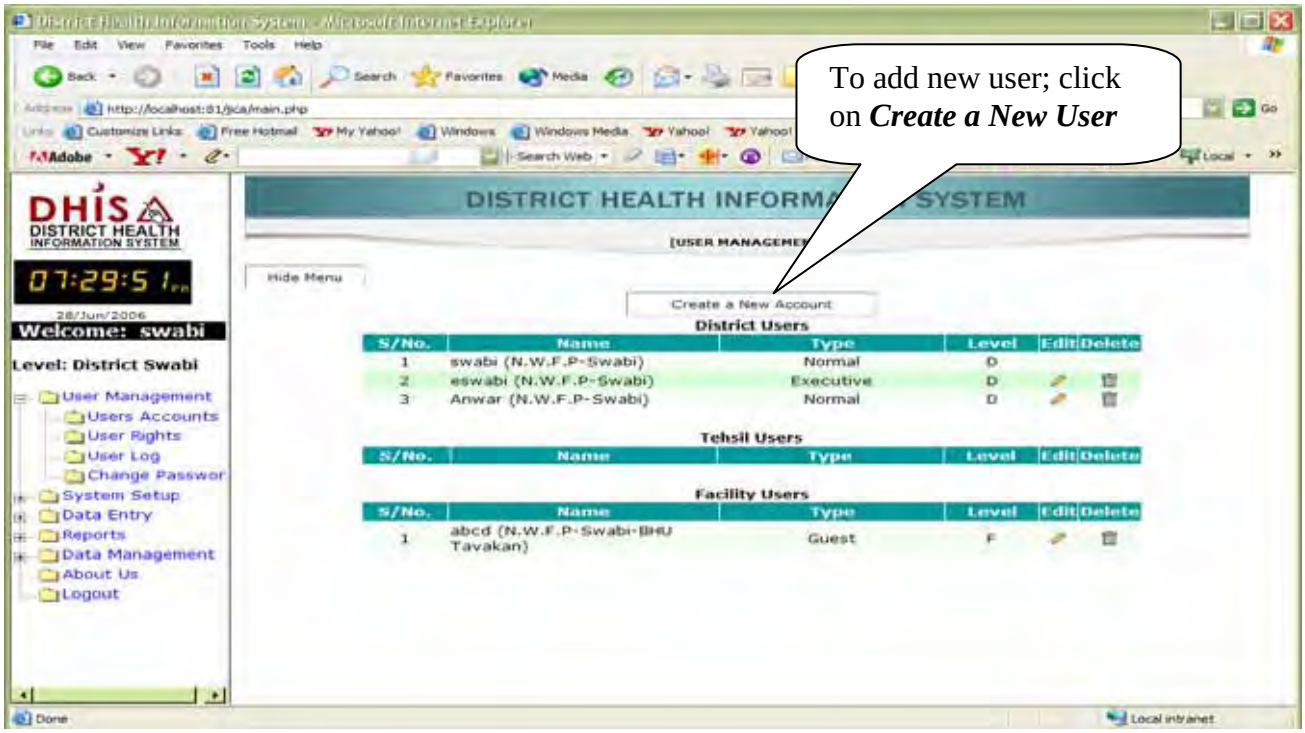


Figure 5

3. Provide information for the new user and save

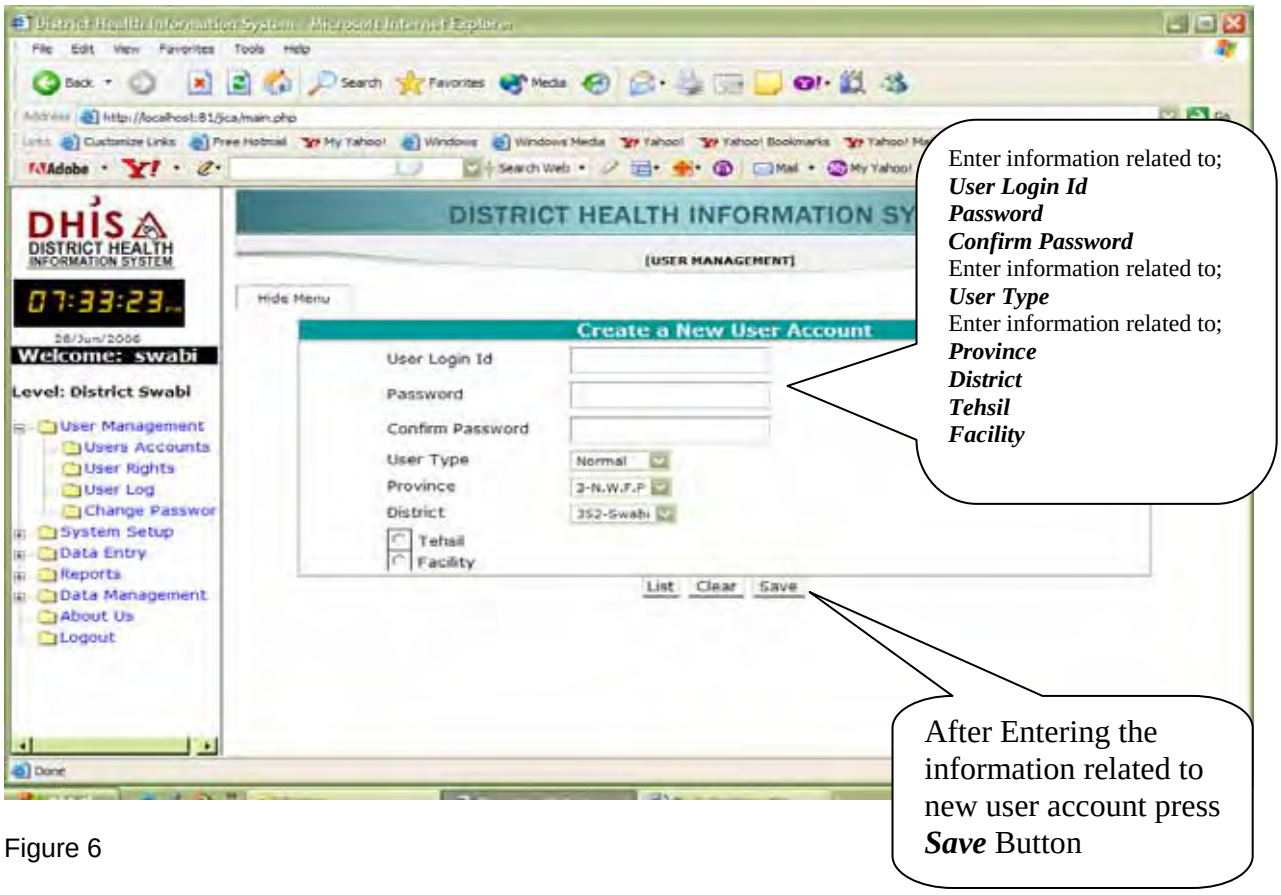


Figure 6

User Rights

To provide or edit rights of existing user follow the following instructions;

1. Select User Rights Option

Figure 7

2. Select User Rights Option

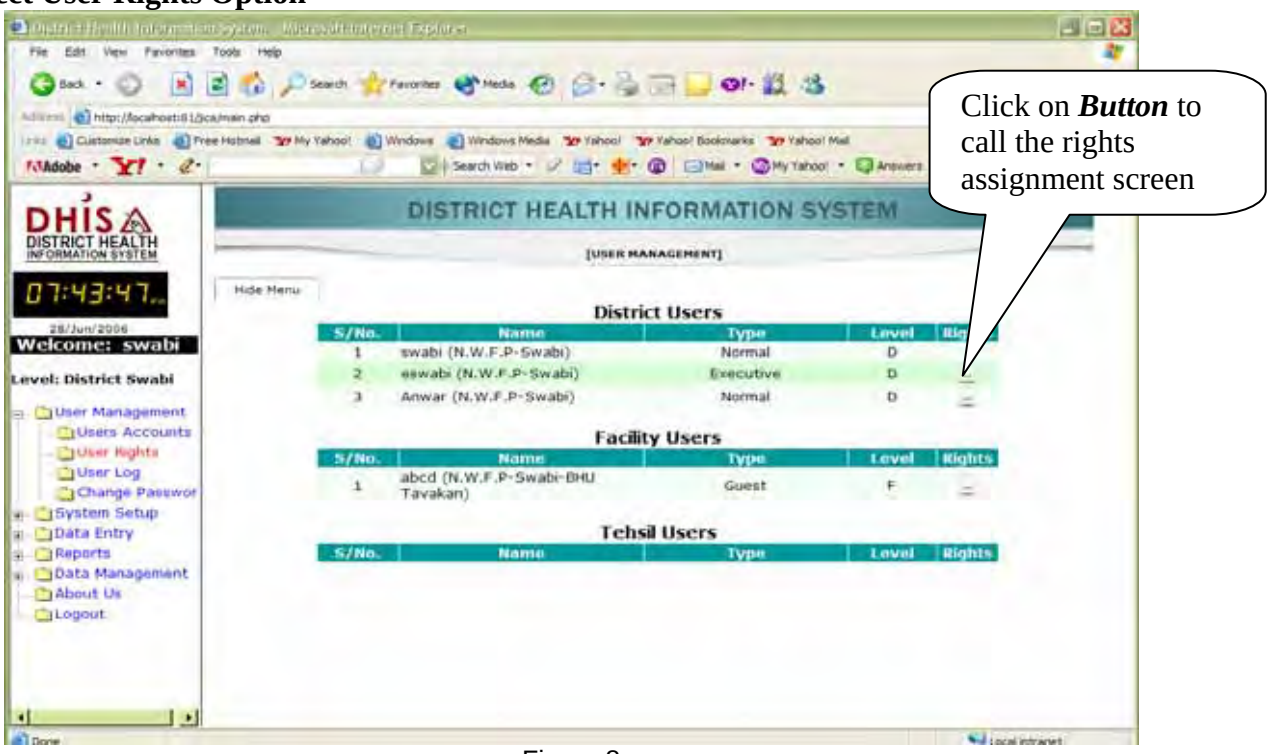


Figure 8

3. Assign User Rights

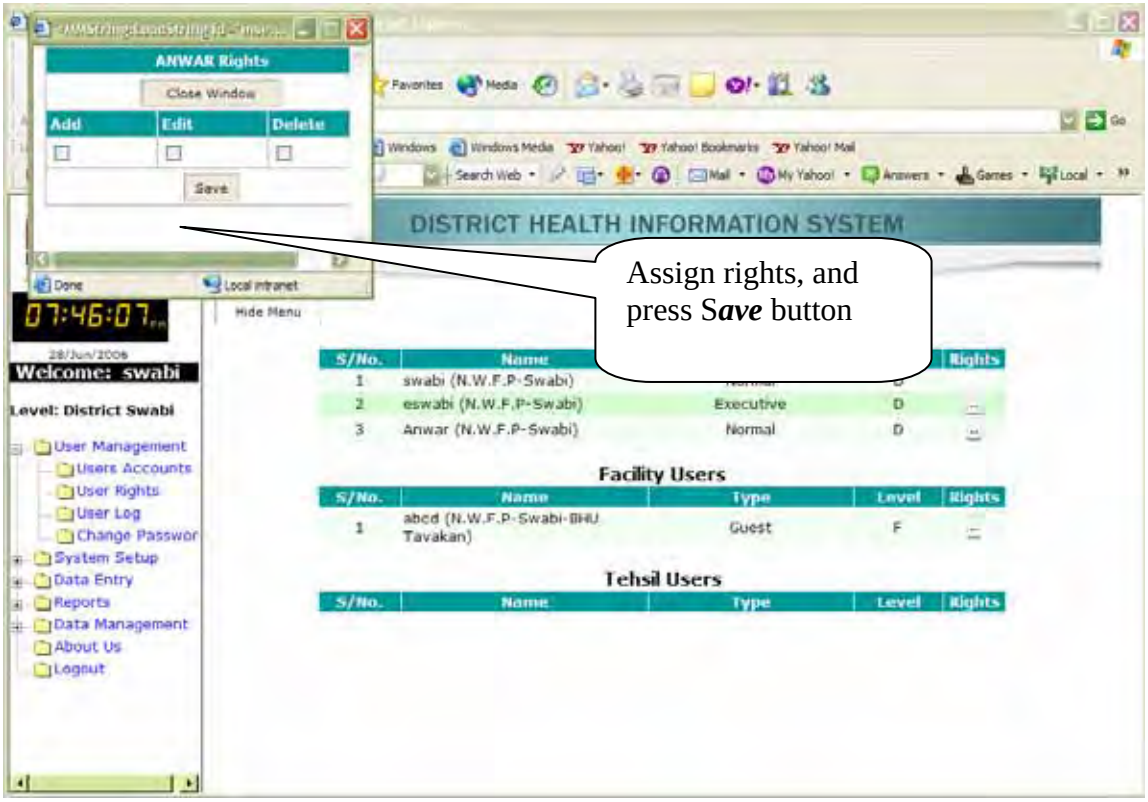
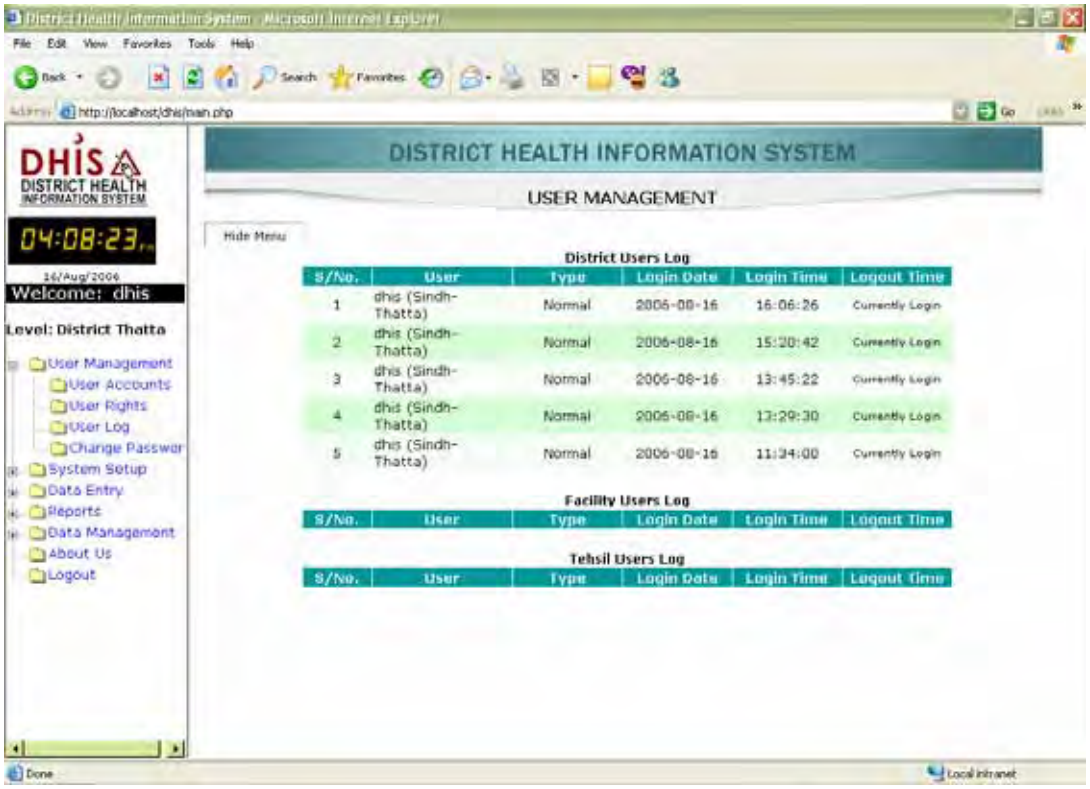


Figure 9

User Log



Change Password

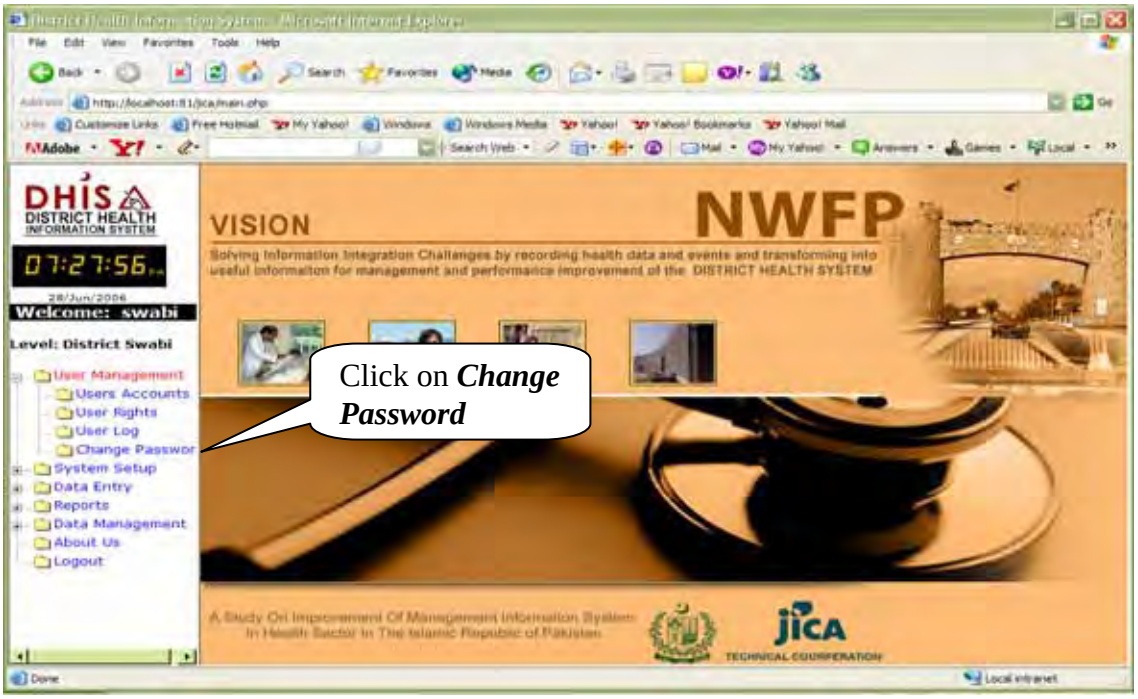


Figure 10

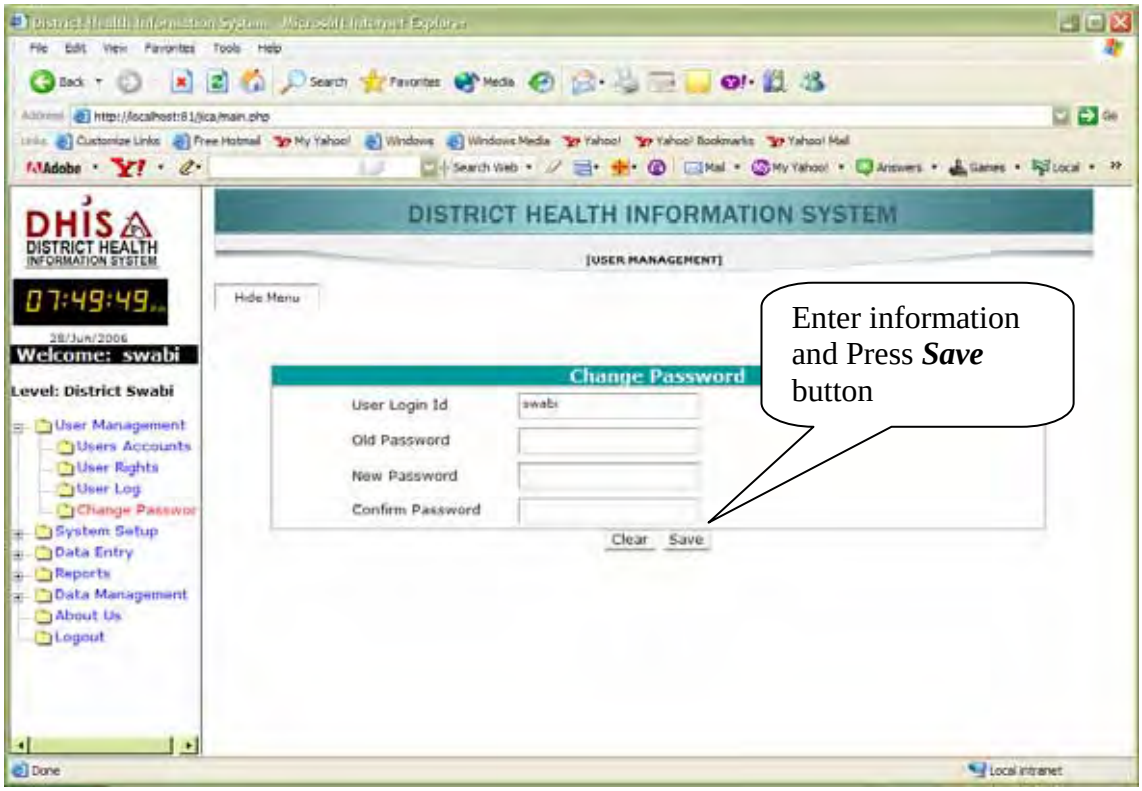


Figure 11

Enter Monthly Report

Activities	Steps Involved	Action	Figure
Data Entry	Click on the + sign against the Data Entry	To call screen; click on ***New Form Entry***	Figure 12,13
New Data Entry	Data Entry → ***Select form for Entry***	Data Entry for will show. Enter Monthly Data	Figure 14,15,16,17
Edit Existing Monthly Report	Data Entry → ***Edit Existing Form***	Select Facility for editing	Figure 18,19,20,21,22

Enter Monthly Report

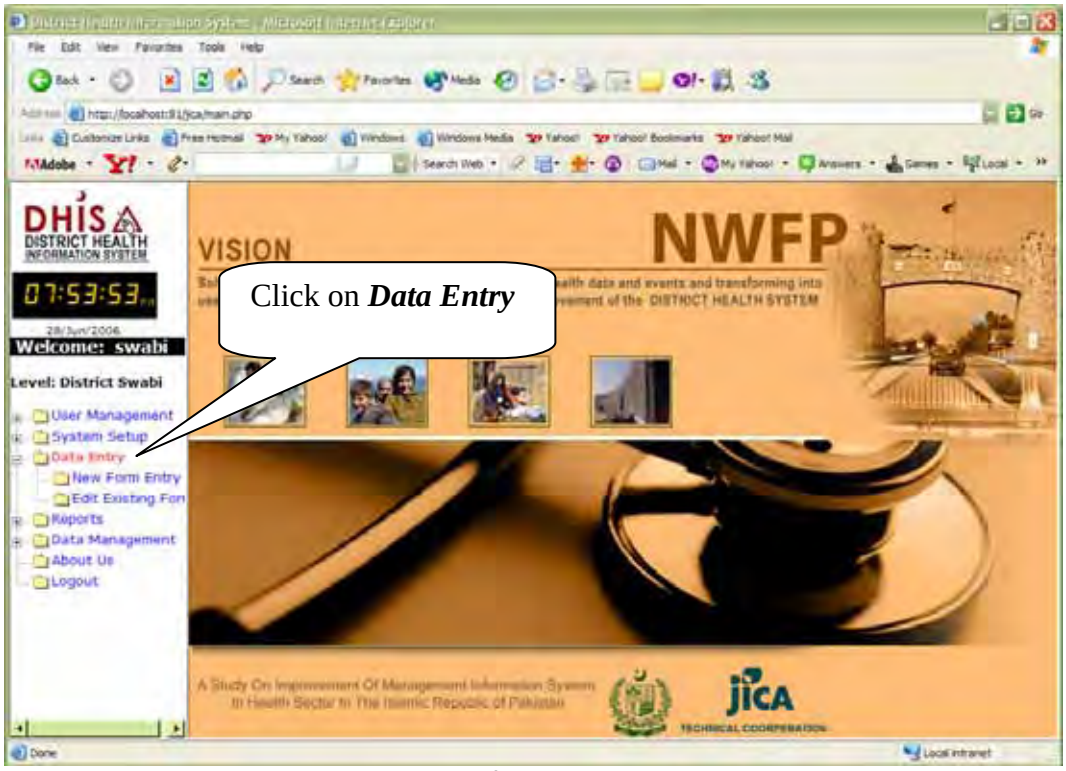


Figure 12

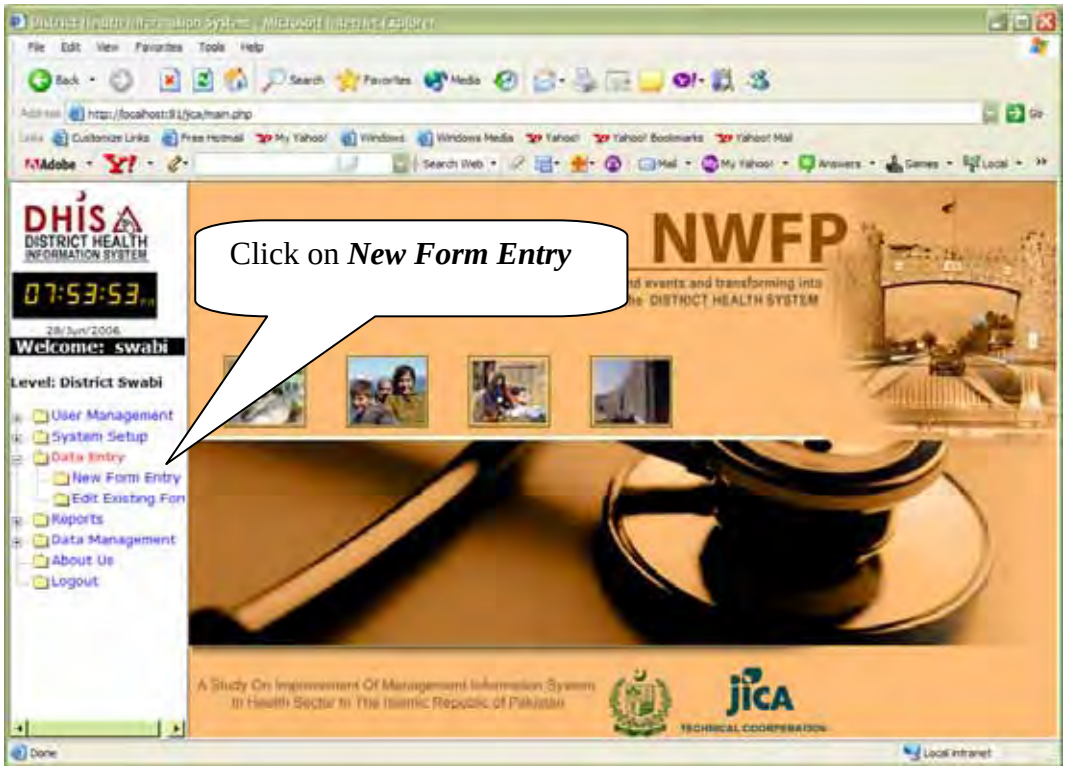


Figure 13

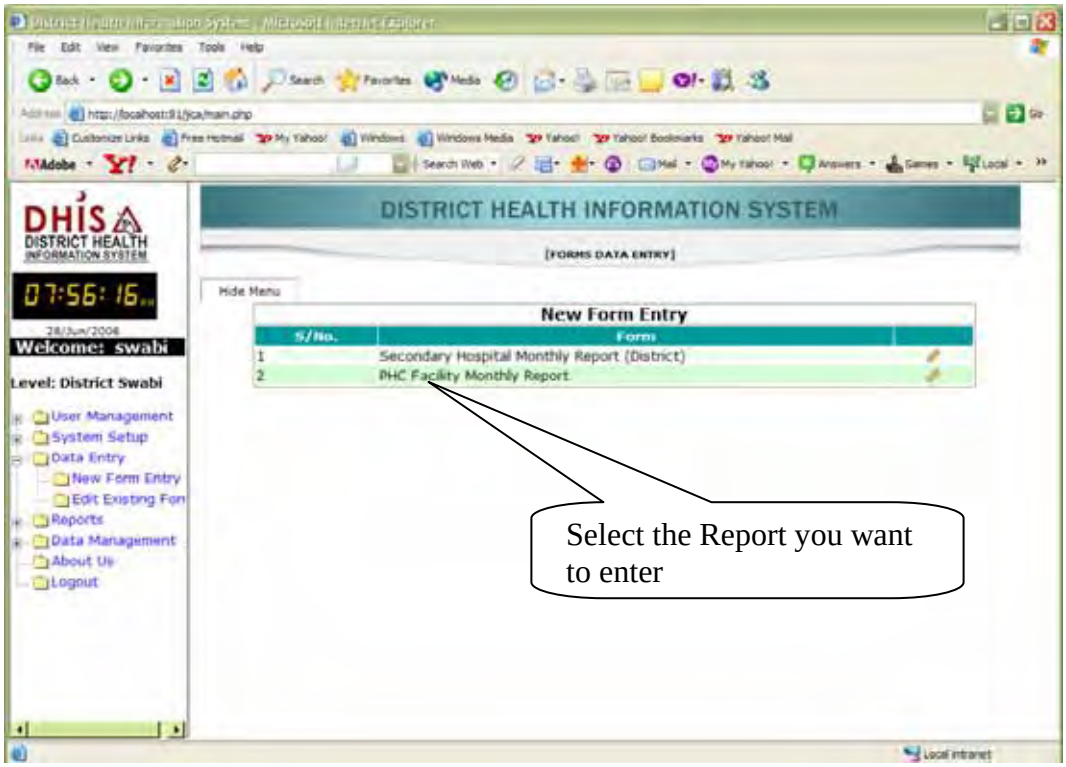


Figure 14

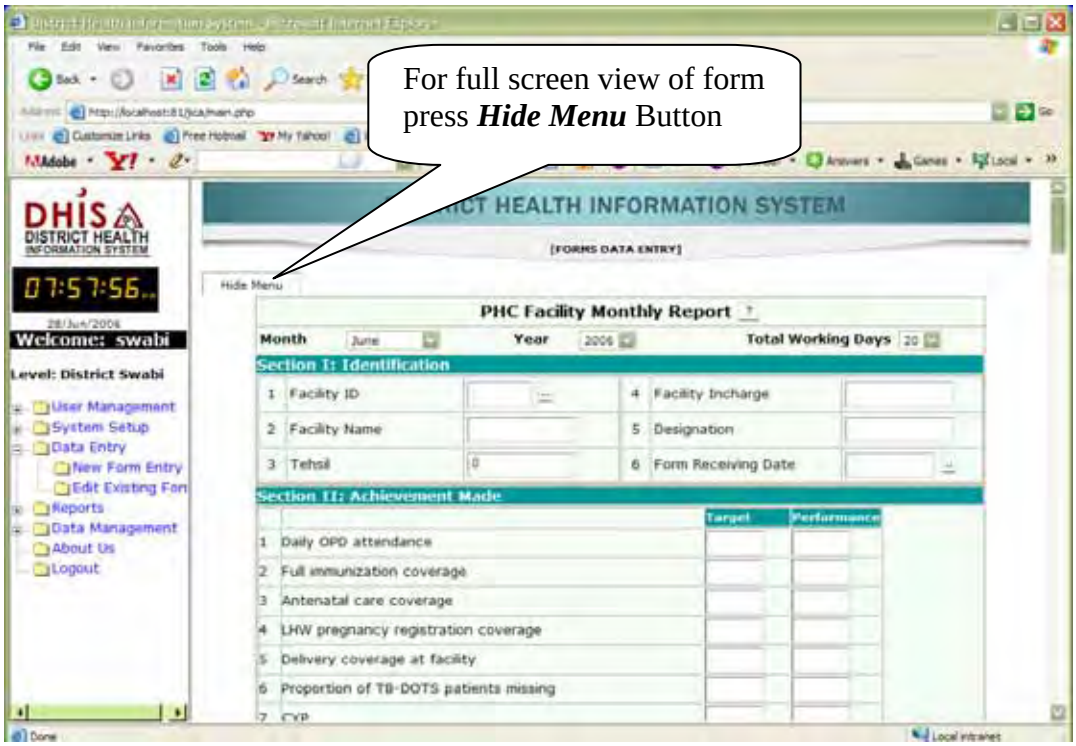


Figure 15

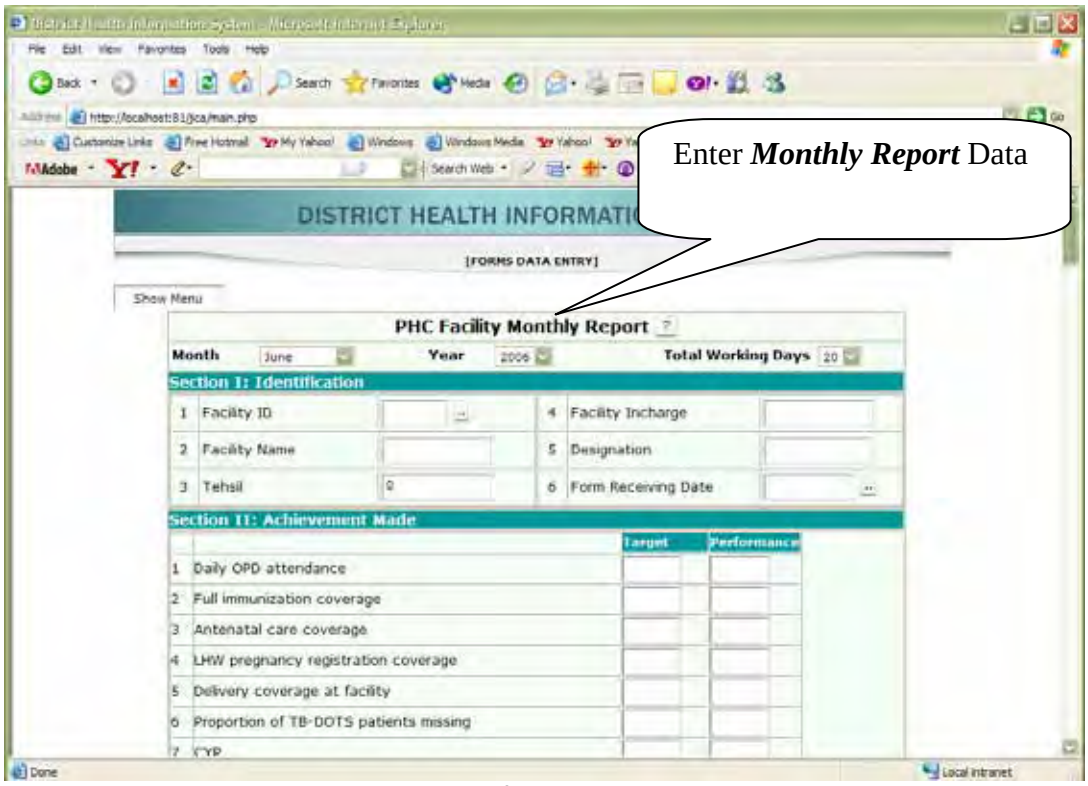


Figure 16

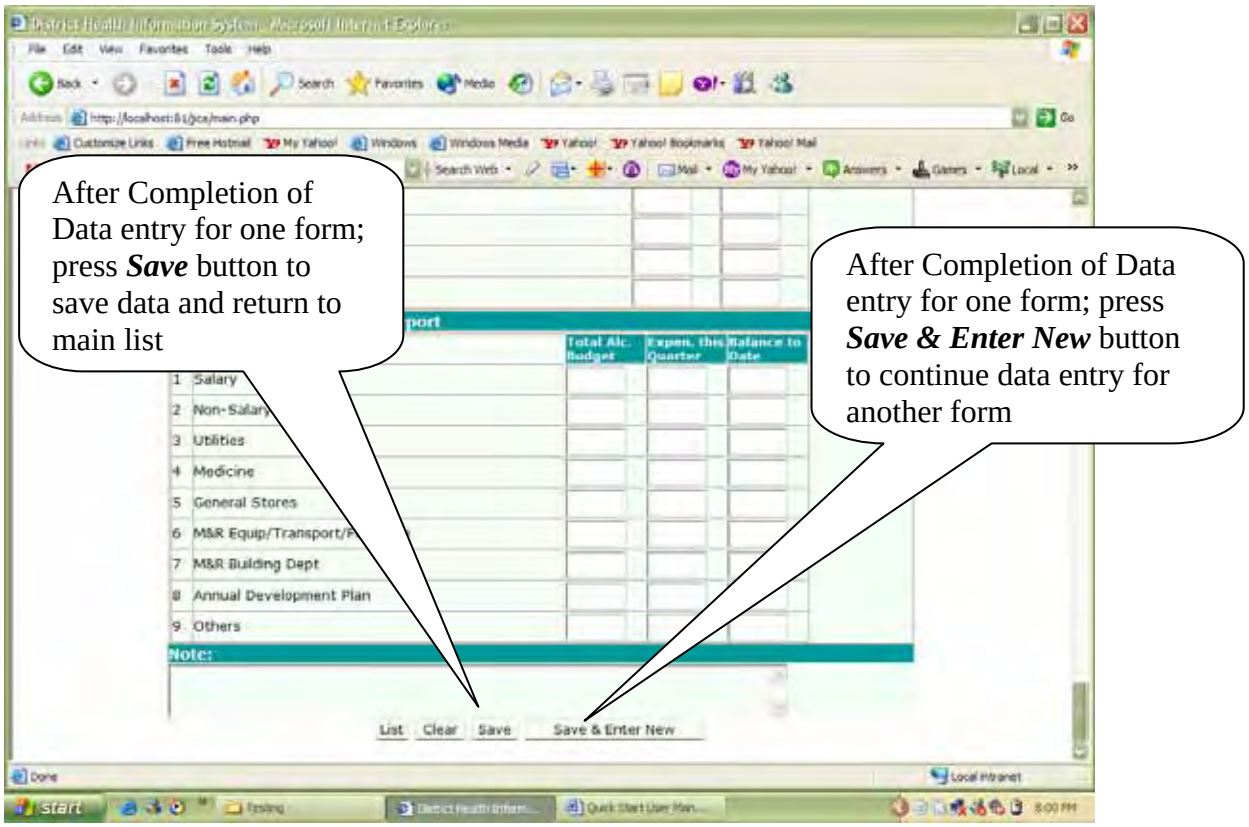


Figure 17

Edit Existing Monthly Report

Figure 18

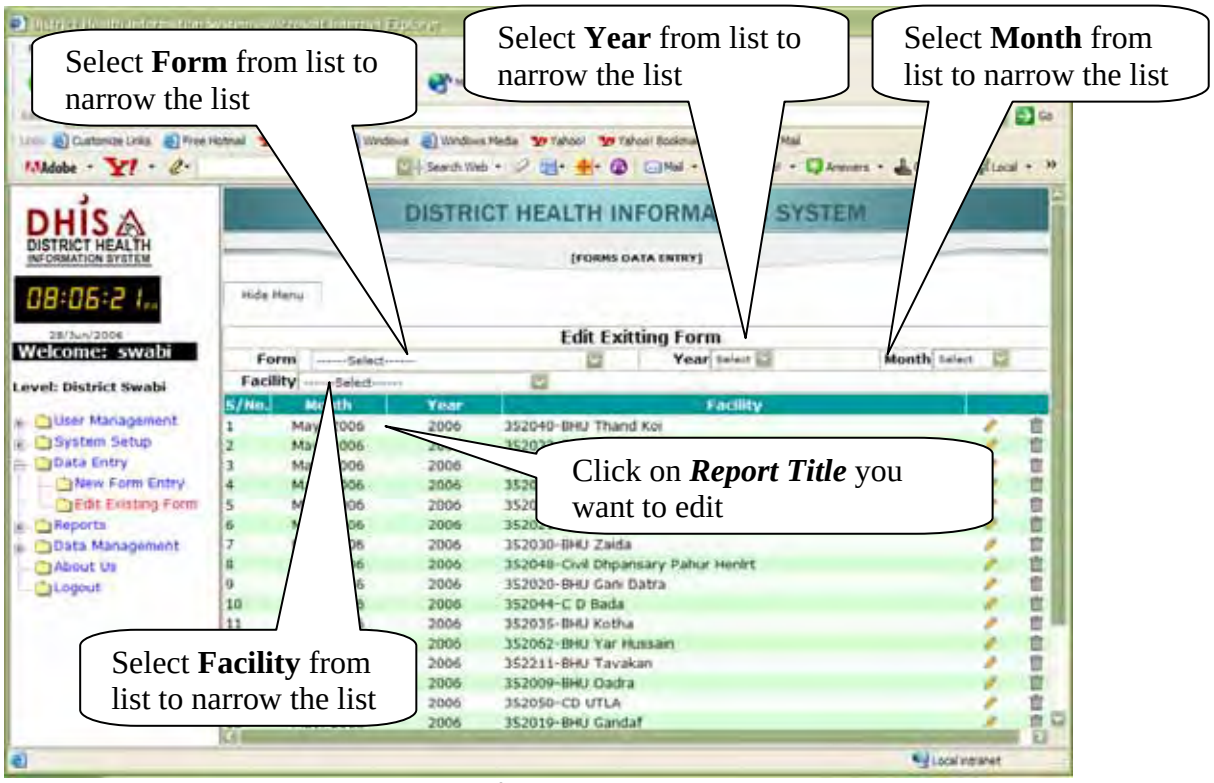


Figure 19

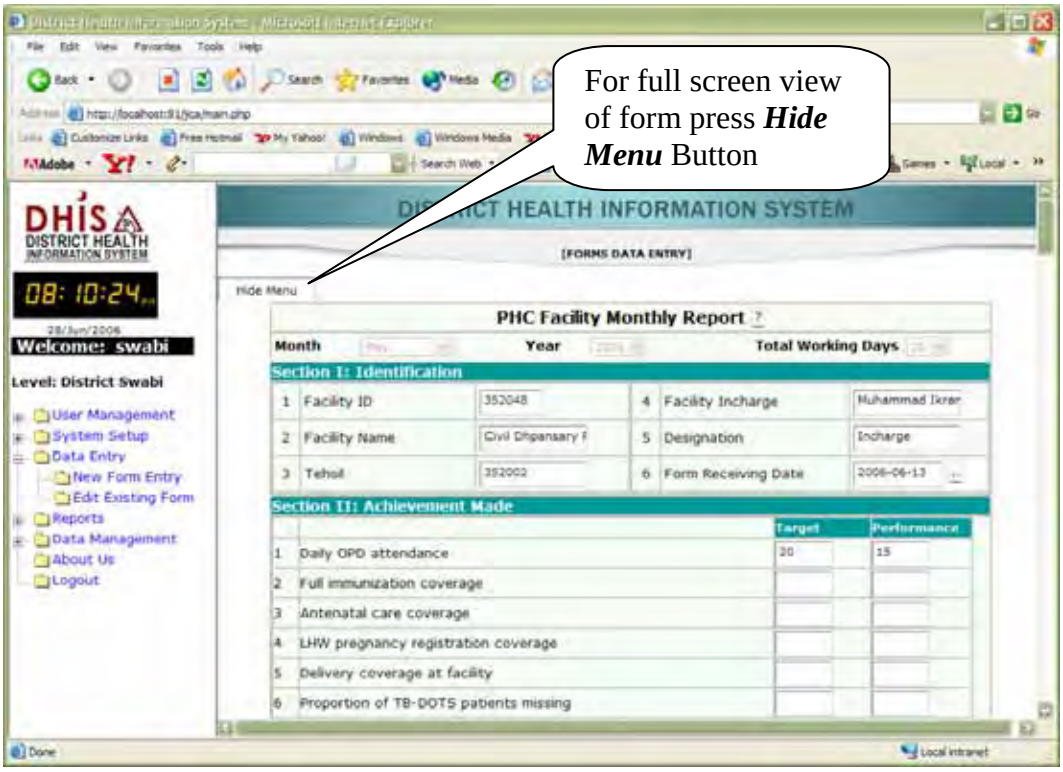


Figure 20

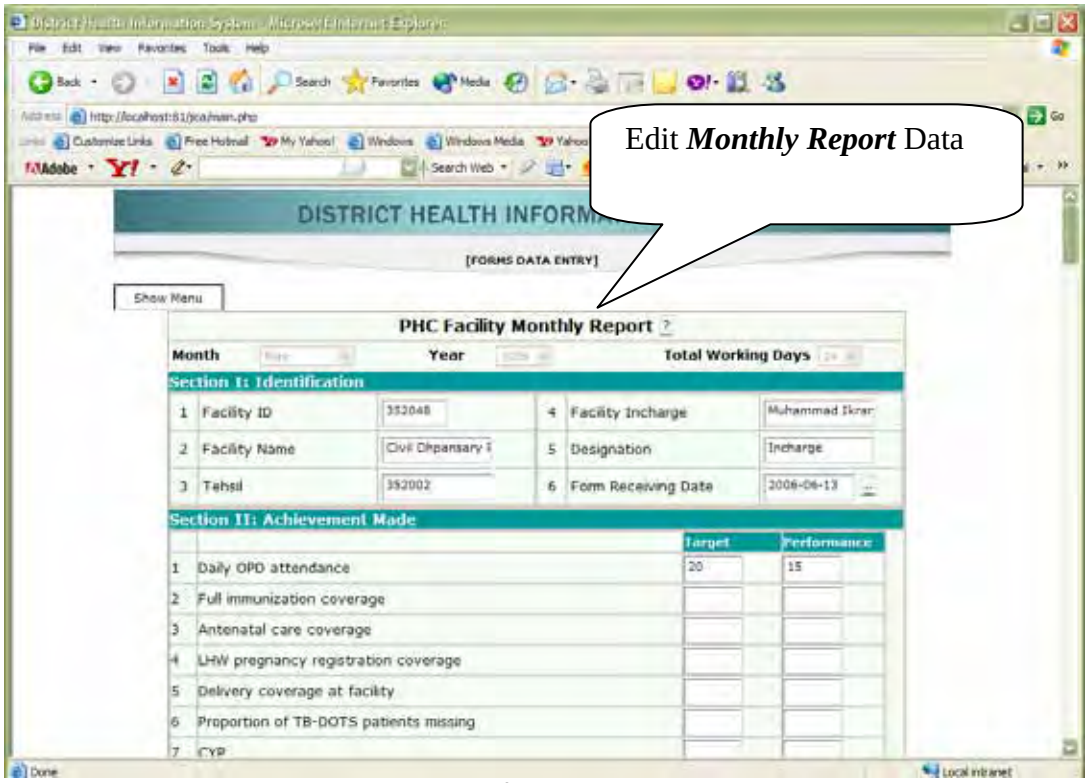


Figure 21

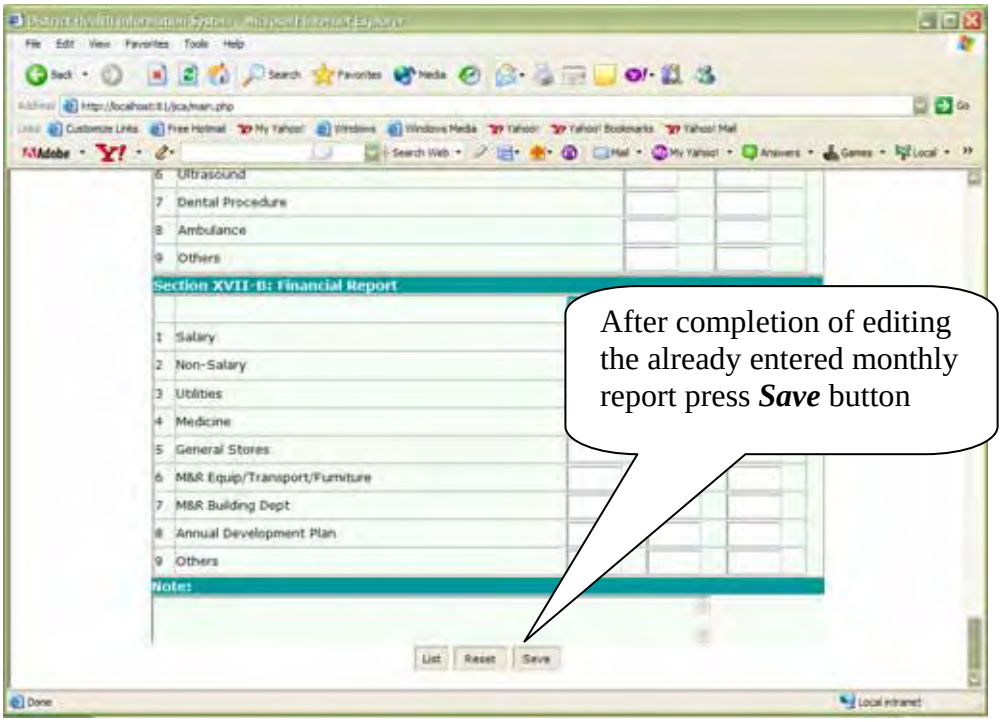

6 Ultrasound
7 Dental Procedure
8 Ambulance
9 Others
Section XVII-B: Financial Report
1 Salary
2 Non-Salary
3 Utilities
4 Medicine
5 General Stores
6 M&R Equip/Transport/Furniture
7 M&R Building Dept
8 Annual Development Plan
9 Others
Note:
List
Reset
Save
After completion of editing the already entered monthly report press ***Save*** button

Figure 22

Reports.

Activities	Steps Involved	Action	Figure
Monthly Reports	Reports→Print Monthly Report	Select the Criteria and press preview button to take print out.	Figure 24
Aggregated Report	Reports→Print Monthly Report	• Consolidated Report (Province) • Consolidated Report (District) • Consolidated Report (Facility)	Figure 24
Printing Options	Reports→Print Monthly Report→ Preview	• Click to Close to Close Report • Click Print to sent to printer • Click on ***PDF*** to convert in to PDF and save on your computer	Figure 25
Indicator Based Report	Reports → ***Indicator Based Report***	Select the Criteria and press preview button to take print out.	Figure 26
Printing Options	Reports→ ***Indicator Based Report*** → Preview	• Click to Close to Close Report • Click to Print to sent to printer • Click on ***PDF*** to convert in to PDF and save on your computer	Figure 27

Take Reports

Figure 23

Monthly Report Printing

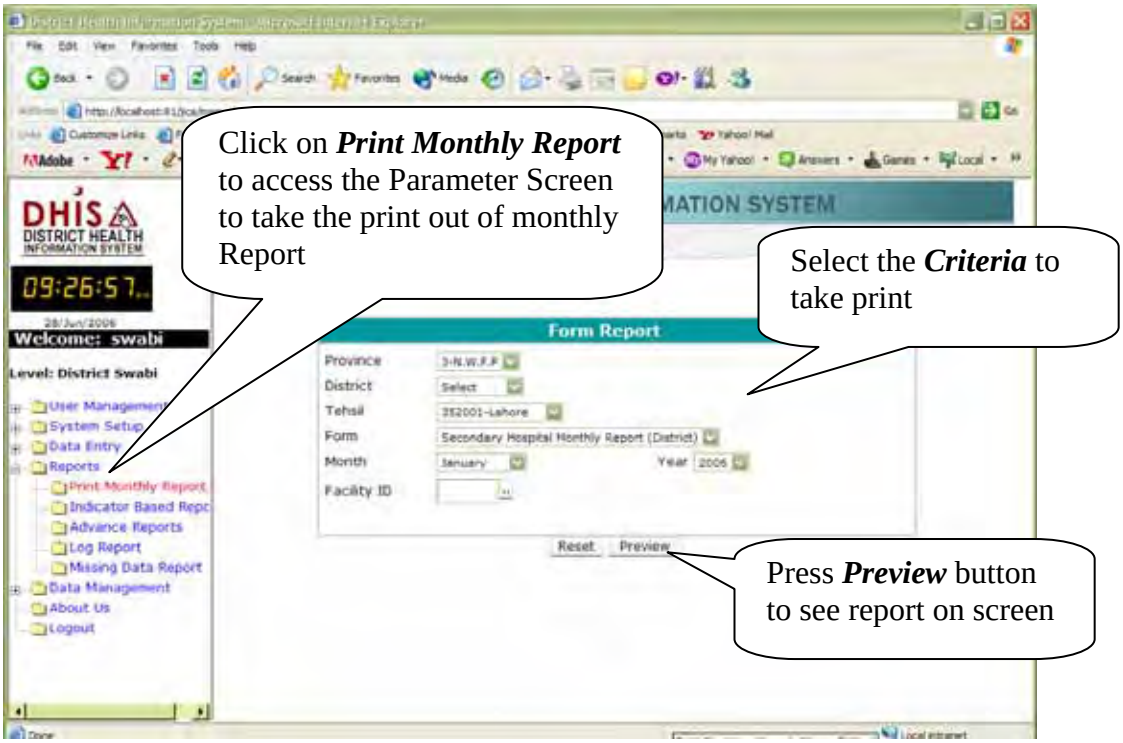


Figure 24

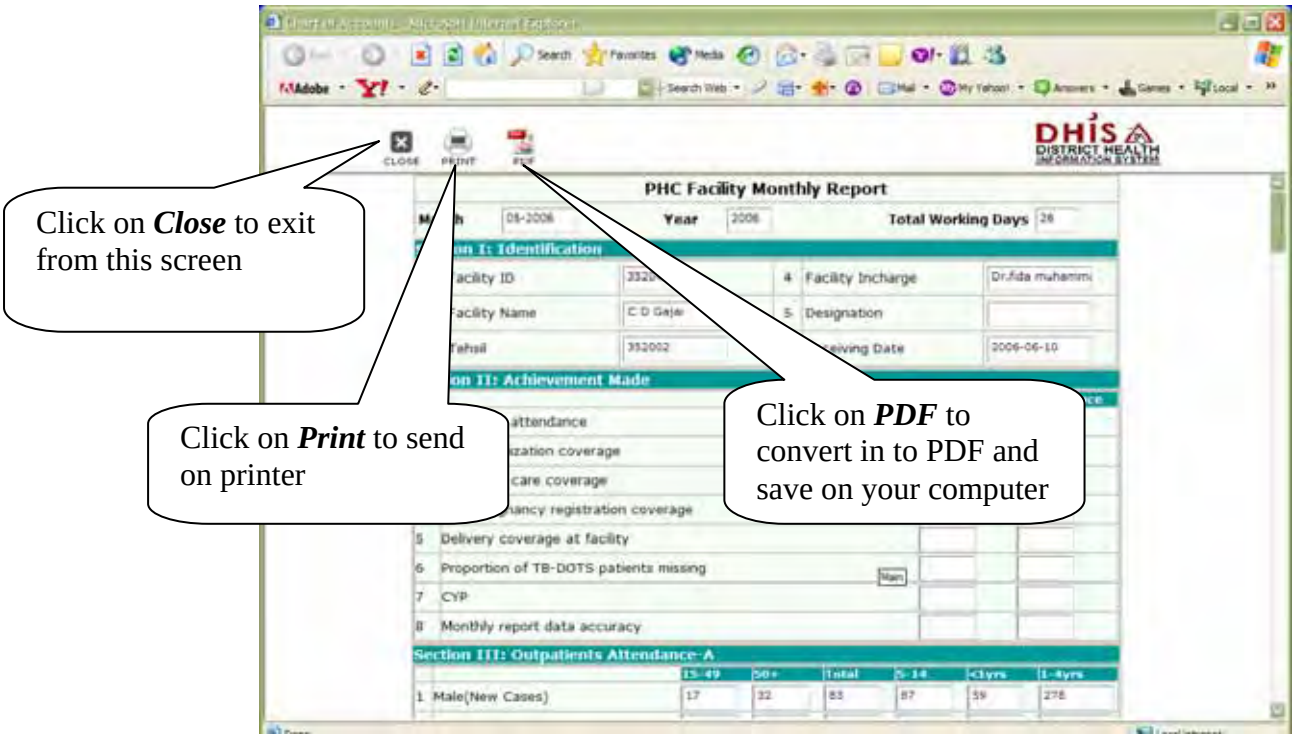


Figure 25

Indicator Based Report Printing

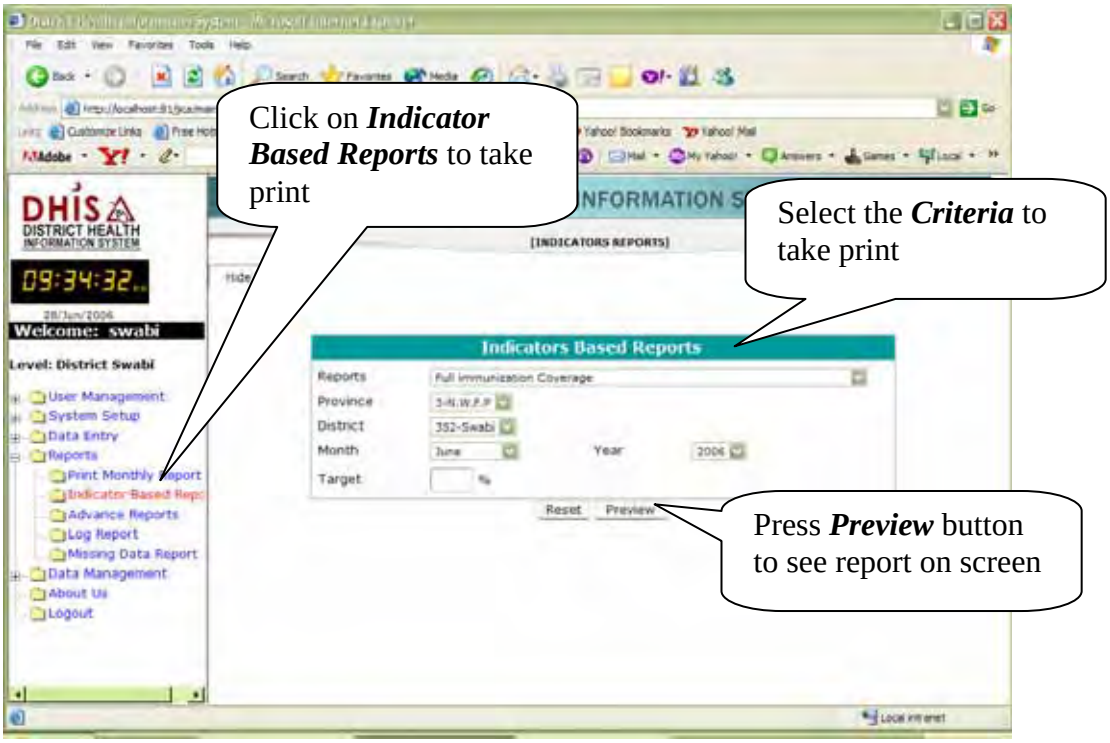


Figure 26

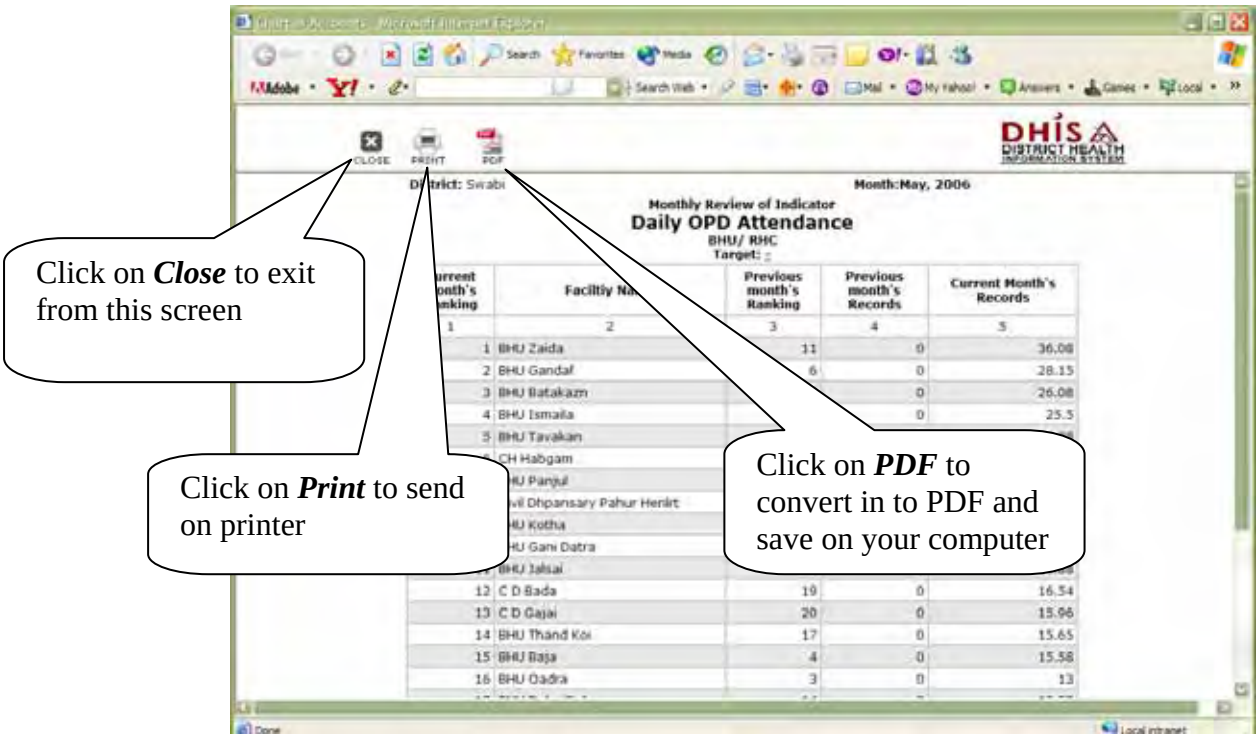


Figure 27

Data Management

Activities	Steps Involved	Action	Figure
Save Batch file (Entered Data)	Data Synchronization→upper level synchronization→ Save Batch file (Enter Data)	Click on ***New Batch*** to Create Dump File	Figure 28
Restore Form (New Forms)	Data synchronization→upper level synchronization→ Restore Form(New Form)	• Click on browse to select dump database file • Click on ***Restore*** to merge new forms data	Figure 29
Lower level synchronization (Restore Saved Data)	Data Synchronization→Lower level synchronization→ Restore Saved data	Click on ***Restore*** to restore downloaded data	Figure 30
Save Batch File (New Forms)	Data Synchronization→lower level synchronization→ Create Batch file (New Forms)	Click on ***Download*** to restore downloaded data	Figure 31
Backup Database	Data management → Backup Database	Click on ***Export*** to take backup of all data	Figure 32
Restore Data	Data management → Restore Data	• Click on browse to select backup file • Press import button to restore data	Figure 33
Export Data to Excel	Data management → Export Data to Excel	Select Criteria and Press save preview button to save in excel sheet	Figure 34

Data Management (Upper Level Synchronization)
Save Batch file (Entered Data)

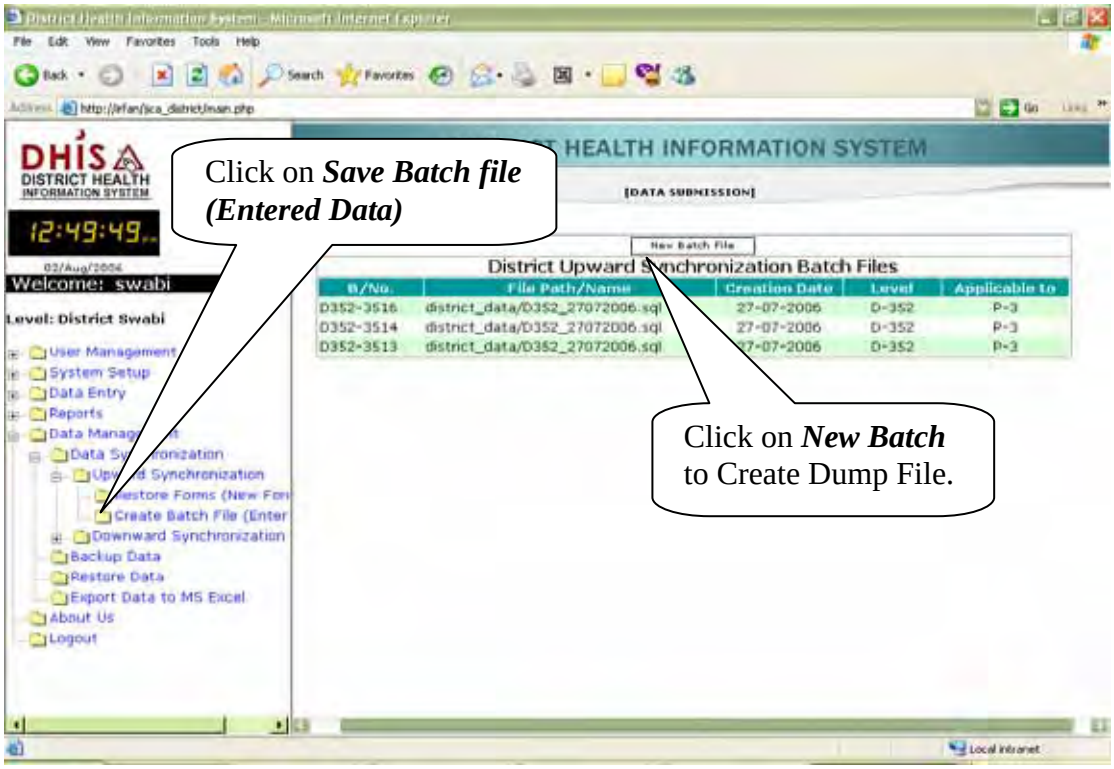


Figure 28

Restore Forms (New Forms)

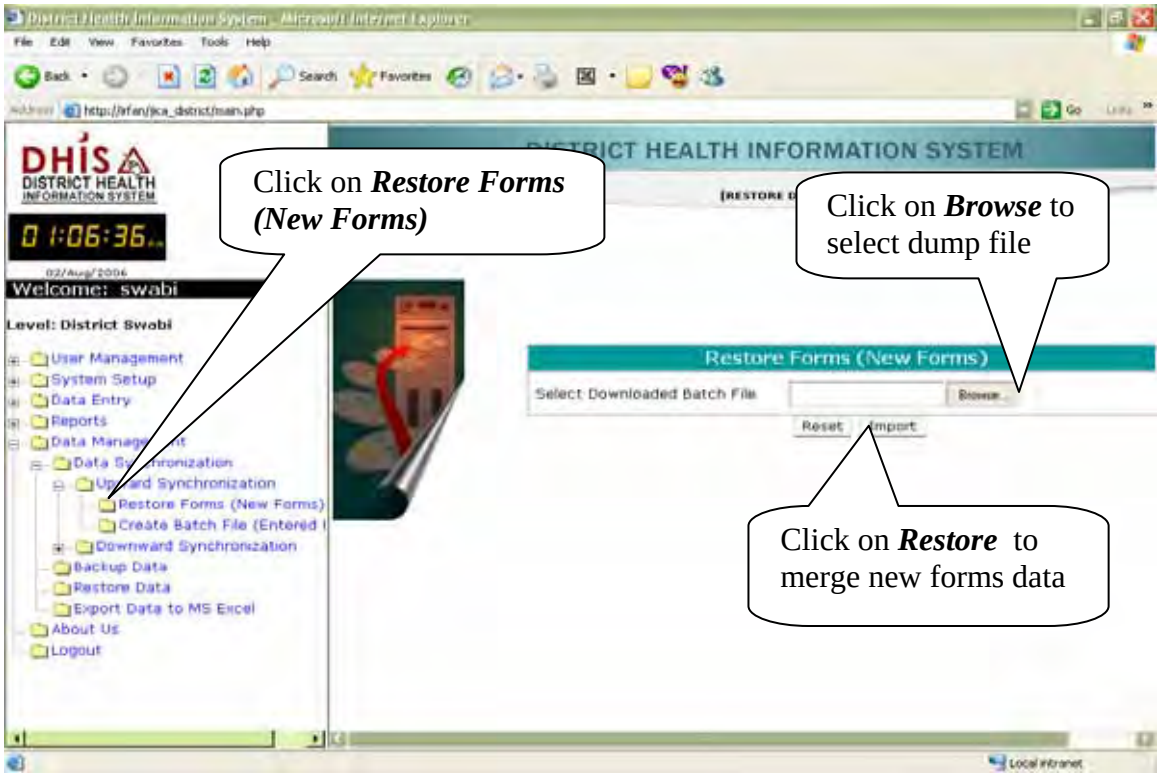


Figure 29

Lower Level synchronization (Restore Saved Data)

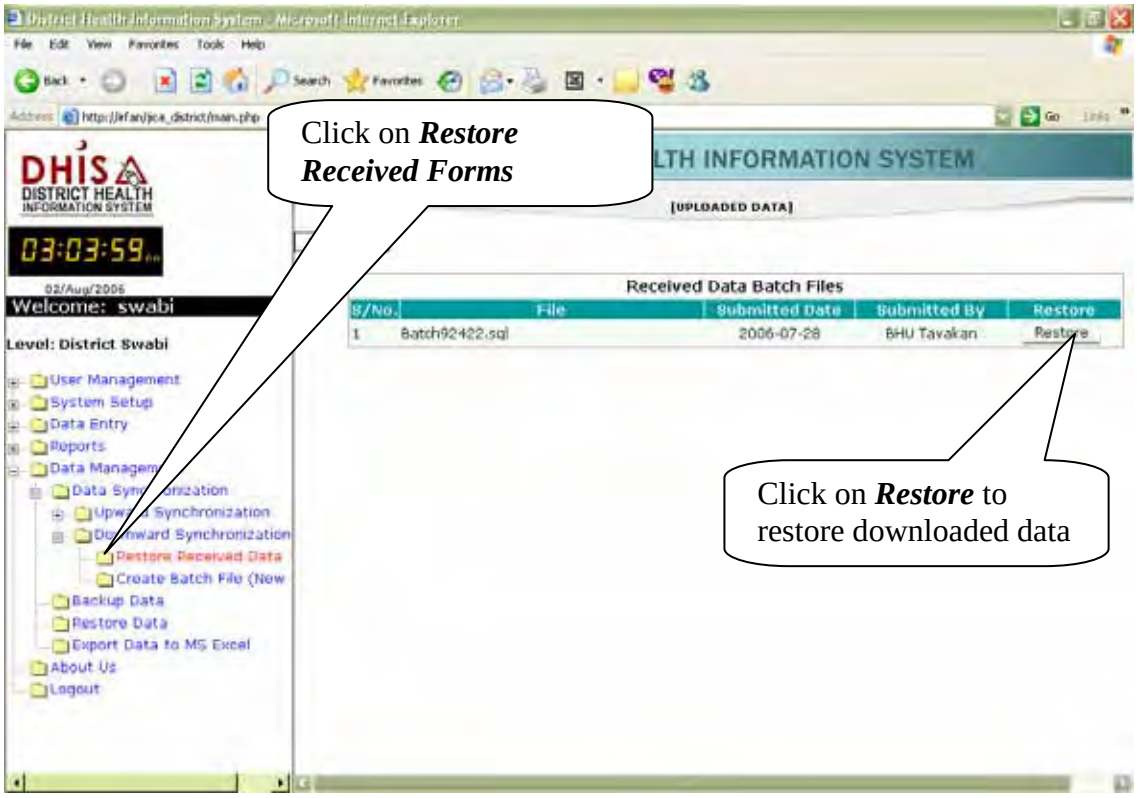


Figure 30

Save Batch File (New Forms)

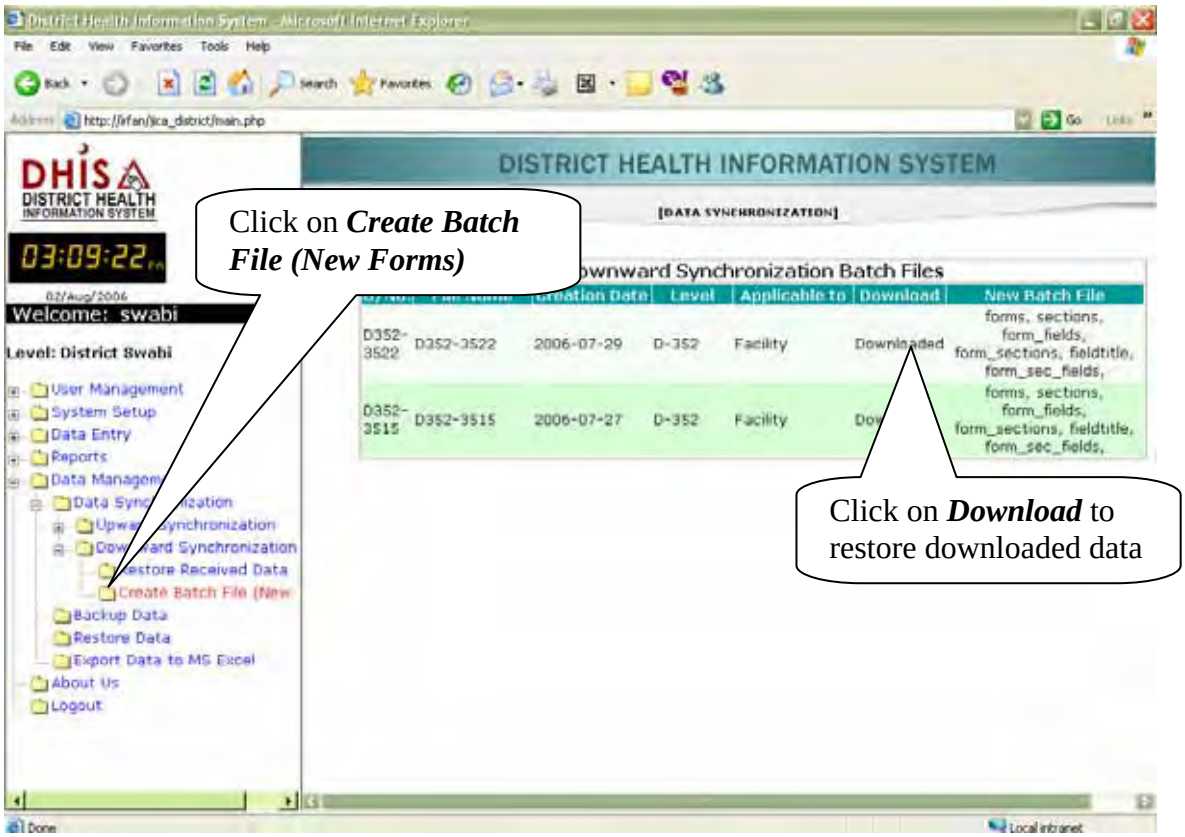


Figure 31

Backup Database.

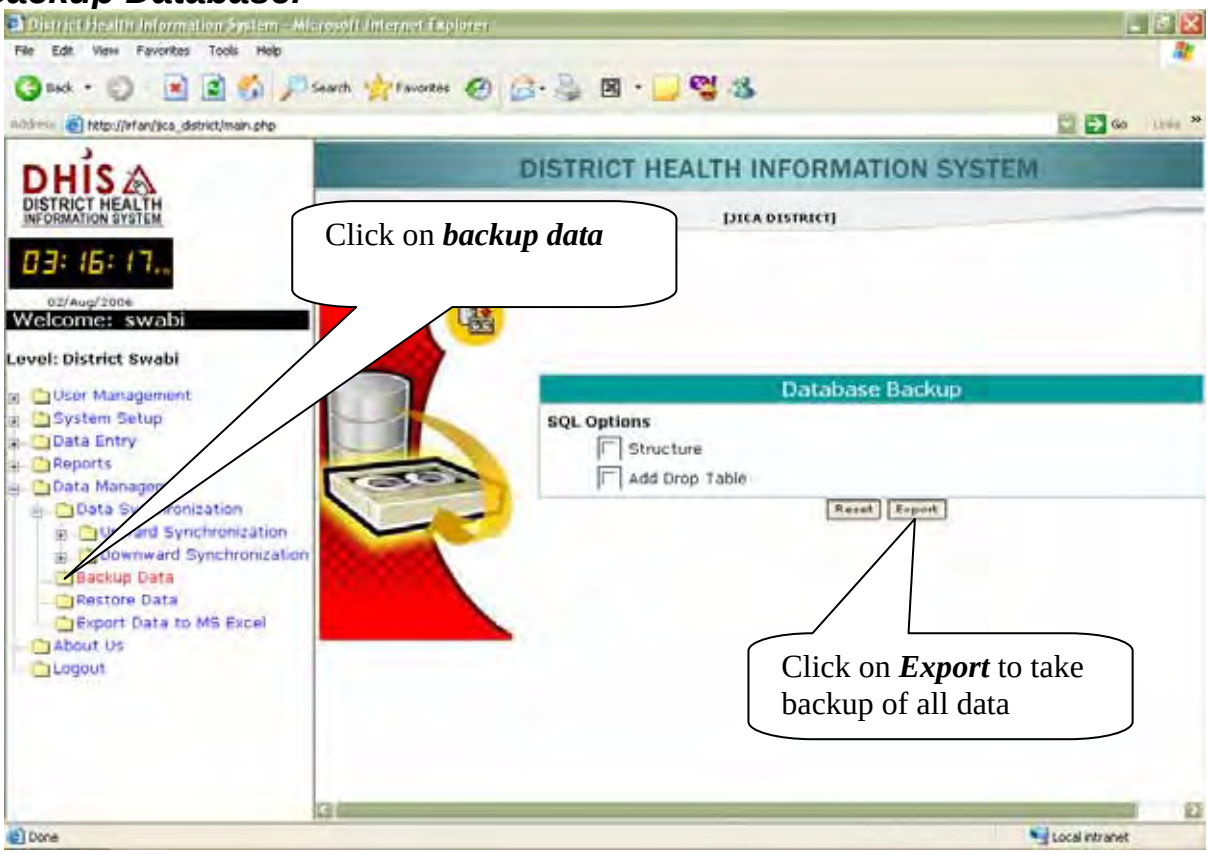


Figure 32

Restore Data.

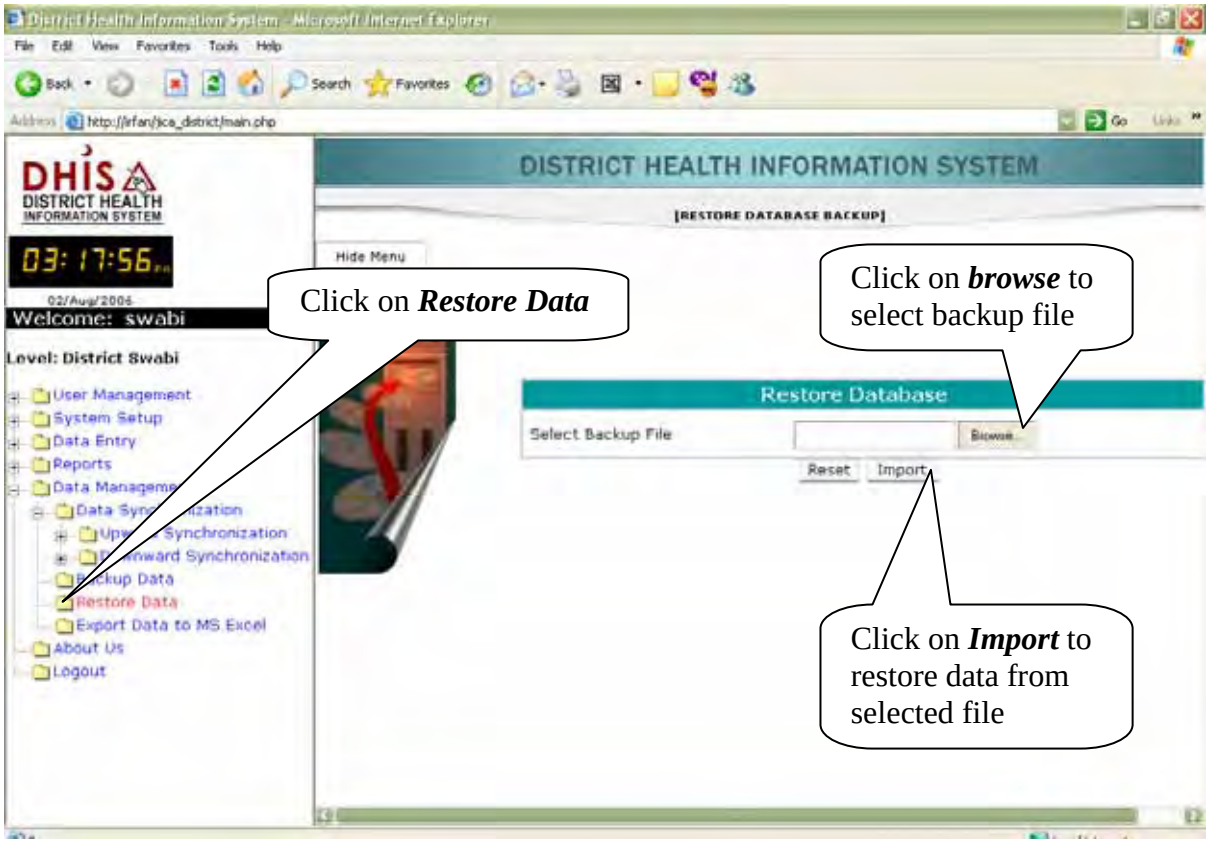


Figure 33

Export Data to Ms-Excel

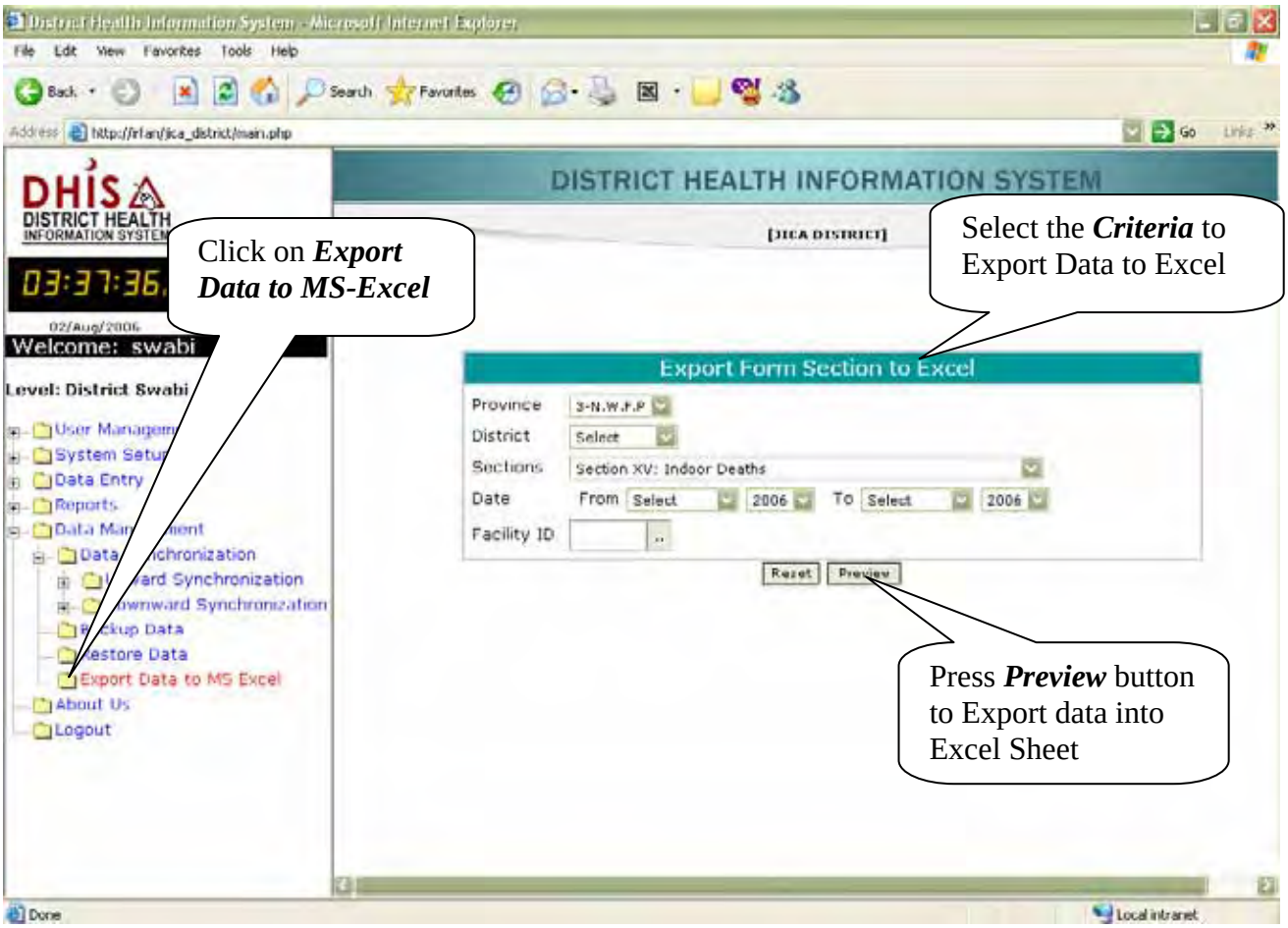


Figure 34

PART II

OPERATIONAL MANUAL

District Health Information System

Sub Contracted Work on Computer System Development

for the Study on

Improvement of Management Information System in Health Sector in The Islamic Republic of Pakistan

Operational Manual

Preface

Welcome to Release DHIS 3.0 of the *DHIS.* This user's guide includes the information you need to work with DHIS effectively. It contains detailed information about the following:

- Overview
- Specific tasks you can accomplish using DHIS
- How to use DHIS System
- DHIS reports, listings & feedbacks
- DHIS System setup
- DHIS Data Management

This preface explains how this user's guide is organized and introduces other sources of information that can help you.

About This User's Manual

This manual is the primary source of information about DHIS System. It contains overviews as well as task and reference information. This guide includes the following chapters:

		Page
Chapter 1	**Introduction to DHIS:** describes the overview of DHIS.	4
Chapter 2	**DHIS Login:** describes how to login in the system to start work.	8
Chapter 3	**User Management:** describes the user management and security tasks for designing user setup.	11
Chapter 4	**System Setup:** describes the tasks need to be done before starting use of DHIS software.	16
Chapter 5	**Monthly Forms Data Entry:** describes the task to enter various types of data and modify existing data etc.	47
Chapter 6	**Routine Reports:** how to get the Reports of DHIS based on entered data etc.	50
Chapter 7	**Indicator Reports:** how to get the Reports of DHIS based on entered data etc.	54
Chapter 8	**Advance Reports:** how to get the Reports of DHIS based on entered data etc.	56
Chapter 9	**Executive Dashboard:** how to use the executive dashboard for managers.	59
Chapter 10	**Data Synchronization:** describes the all the operational activities related to database (e.g Data Backup, Data Restore, Data submission and receiving).	61
Chapter 11	**Data Uploading/Downloading:** how to upload batch file to Upper level.	66
Chapter 12	**Trouble shooting:** how to handle the problem in case of any trouble or disorder.	70

Assumptions

This guide assumes that you have a:

1. Working knowledge of the principles and customary practices of your activity area.
2. It also assumes you have a basic understanding of manual system of the DHIS:
3. DHIS Reports, your organizations reporting process and the flow of information from your organization's level to the consolidation.
4. The maintenance section of this guide assumes you have a basic understanding of operating system concepts and familiarity with Fedora/Postgre SQL administration (Admin users).

Do Not Use any Database Tools to Modify DHIS System Data.

DHIS system provides powerful graphical interface you can use to create, store, change, and retrieve and maintain information in the database. But if you use Postgre SQL tools to modify DHIS data, you risk destroying the integrity of your data. Because the application tables are interrelated, any change you make using an application window can update many tables at once. But when you modify Applications data using anything other than DHIS Applications windows, you may change a row in one table without making corresponding changes in related tables. If your tables get out of synchronization with each other, you risk retrieving erroneous information and you risk unpredictable results throughout the Applications. When you use DHIS Applications windows to modify your data, the system automatically checks that your changes are valid.

Therefore, we STRONGLY RECOMMEND that you never use SQL Editor, database triggers, or any other tool to modify DHIS tables.

Capacity Building

Responsible department should perform capacity building activities for the system users of Federal/Province/Facility Level staff on continues basis, to upgrade the knowledge to latest technologies.

About AZM

AZM Computer Services (Pvt) Ltd has been in software consultancy and development for the past 25 years. AZM develops and markets an integrated line of software products comprising of more than 15 software modules for financial management, inventory control, procurement, manufacturing, cost accounting, assets management, human resources, and sales and service management, preventive maintenance. AZM products are available for minicomputers, personal computers, network computer**s,** and allowing organizations to integrate different computers, different networks, and even different database management systems, into a single, unified computing and information resource. For more information about AZM please visit www.azm.com.pk

Thank You

Thank you for using DHIS Software and this user's guide. We value your comments and feedback. At the end of this manual is a Reader's Comment Form you can use to

explain what you like or dislike about DHIS Software or this user's guide. Mail your comments to the following address or call us directly at 92-51-2114096-8, or send electronic mail to azm-isb@azm.com.pk

Chapter -1

Introduction to DHIS

Introduction

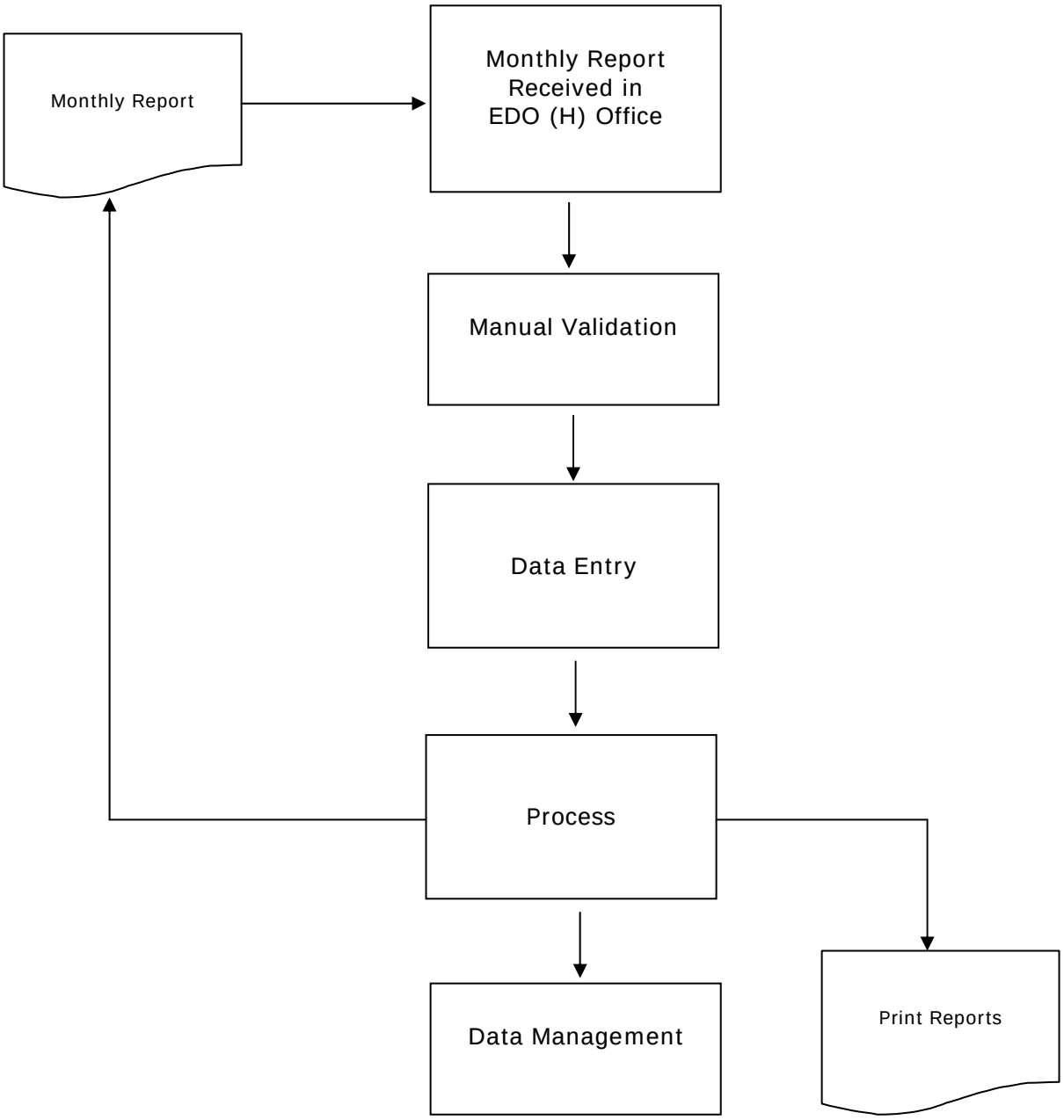
The existing manual/semi computerized information/reporting management system has a fix schedule for up word flow of information at each level i.e. Facility, District, Province and Federal. This flow of information in manual system takes much time to reach from lower tier to upper tier. The ***DHIS*** which corresponds to the current systems would allow the managers to respond proactively to changes in today's competitive business climate. It provides quick and easy implementation; accurate and timely processing of all the transactions, improved decision support through better reporting and analysis. It can greatly increase the operational efficiency of the businesses – an advantage crucial to success in today's fast moving organization arena.

The ***DHIS*** is built upon the principle that all transactions are entered only once, whether at district level or its upper tire. It is a ***multi-location system***, with consolidation of data possible at the provincial/Federal level for reporting month. It is the central repository of all the Facilities activity, maintaining the highest summary level of MIS reporting information from the transaction details supplied by its lower level. All events that have a reporting or monetary impact is ultimately reflected in the DHIS.

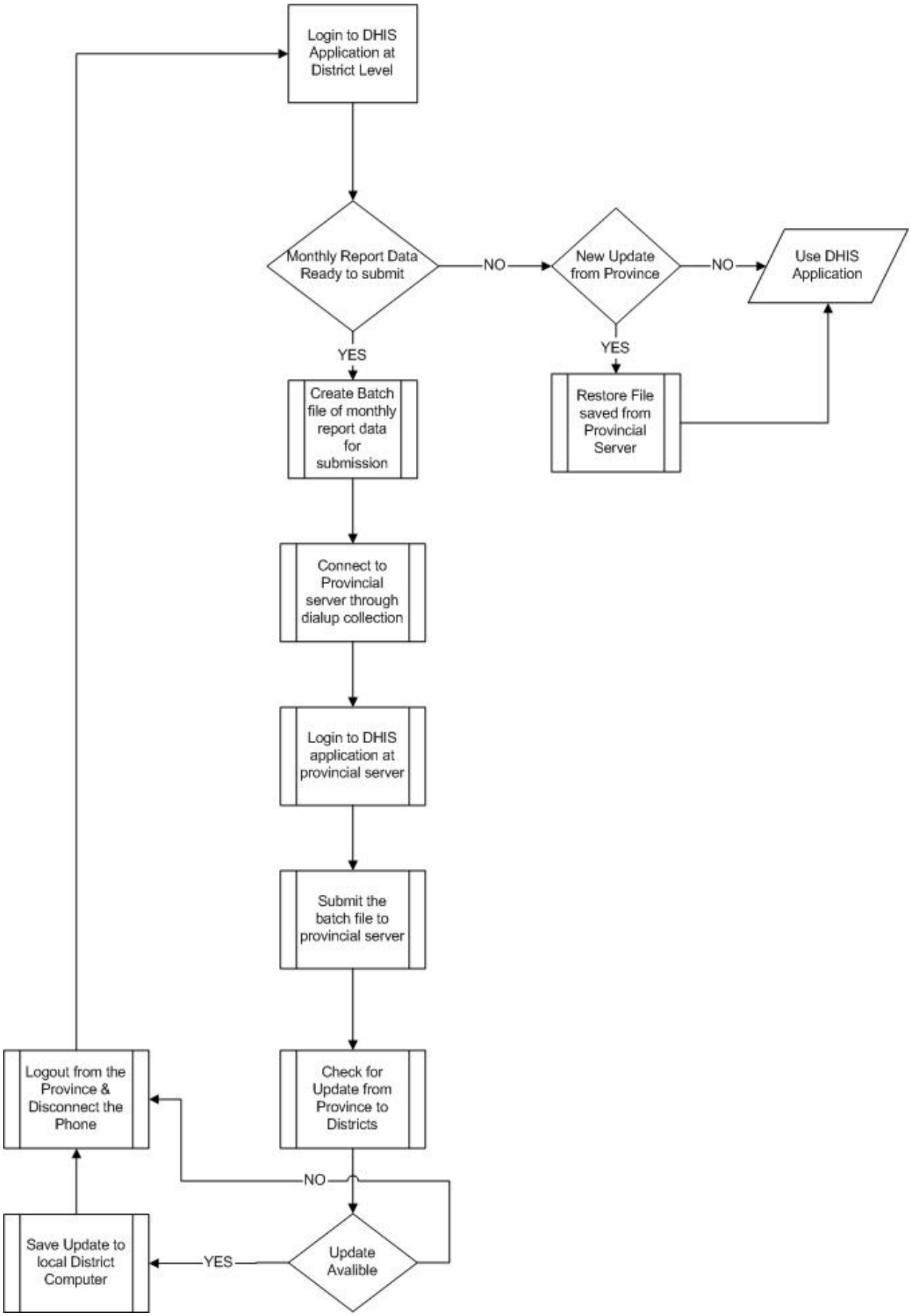
Main features of The DHIS System are:

- ***Open Sources*** Technology
- ***Client-server*** environment.
- ***Online*** as well as batch processing.
- ***Multi-location*** data entry.
- ***Consolidation*** at provincial/federal level for two or more locations.
- ***Multi-year*** data entry.
- ***Form Definition*** to introduce and record local level data collection forms.
- ***Advance Reporting*** to generate user defined reports.
- Screen level ***User rights.***
- ***Laser Printing*** for all outputs.
- ***Exports*** all outputs to Excel and PDF.
- ***Data Backup*** for all Entered Data***.***
- ***Data Restore*** for all saved data***.***
- ***Data Management*** for upper and lower levels.

Monthly Report Operational Work Flow



Data Synchronization Work Flow

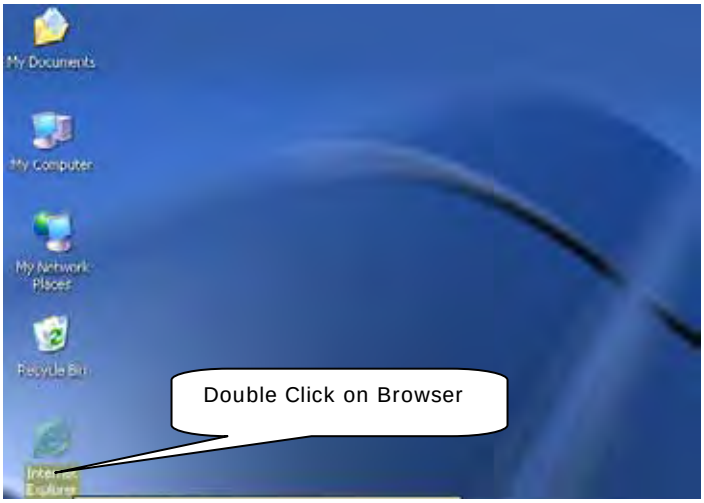


Chapter – 2

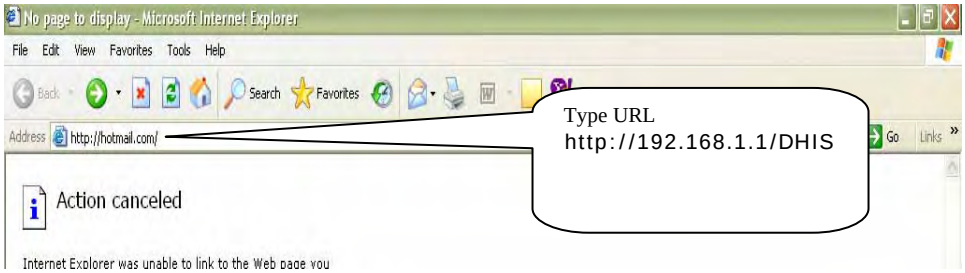
Login to DHIS Application

Login to the Modules

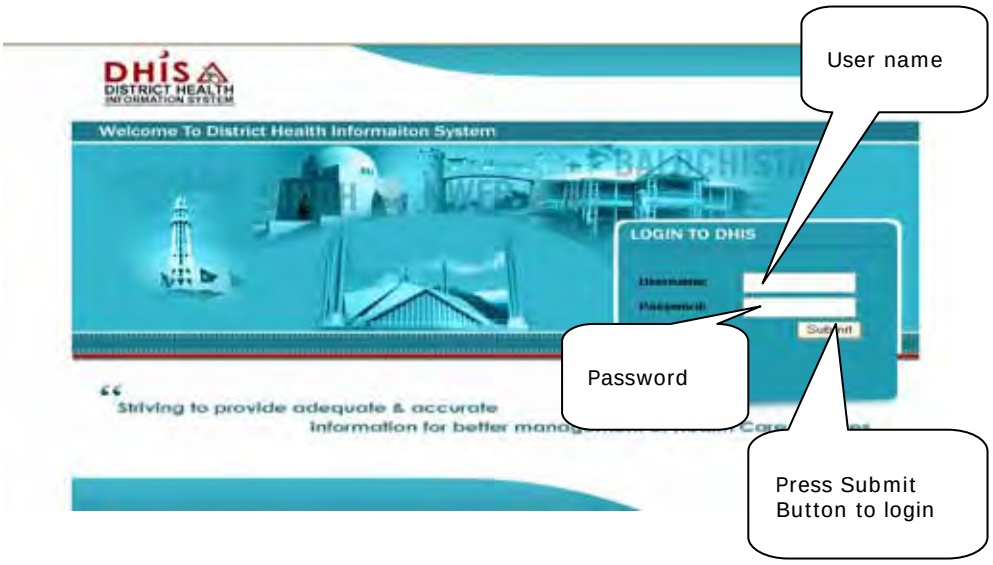
Double Click in browser on desktop.



Type the URL http://192.168.1.1/DHIS or http://[***your-server-name]***/DHIS



Login page will appear in front of you will be for user authentication, following screen will appear for authentication:



Only user with proper user rights and password can login to the system. Incase of invalid user name the following Message box will appear which will show the invalid User name and Pas

Figure: Invalid User or Password

Login name and after providing password will log in to the system. After login in to the system, the main menu will appear in front of you showing the respective province name on main page.

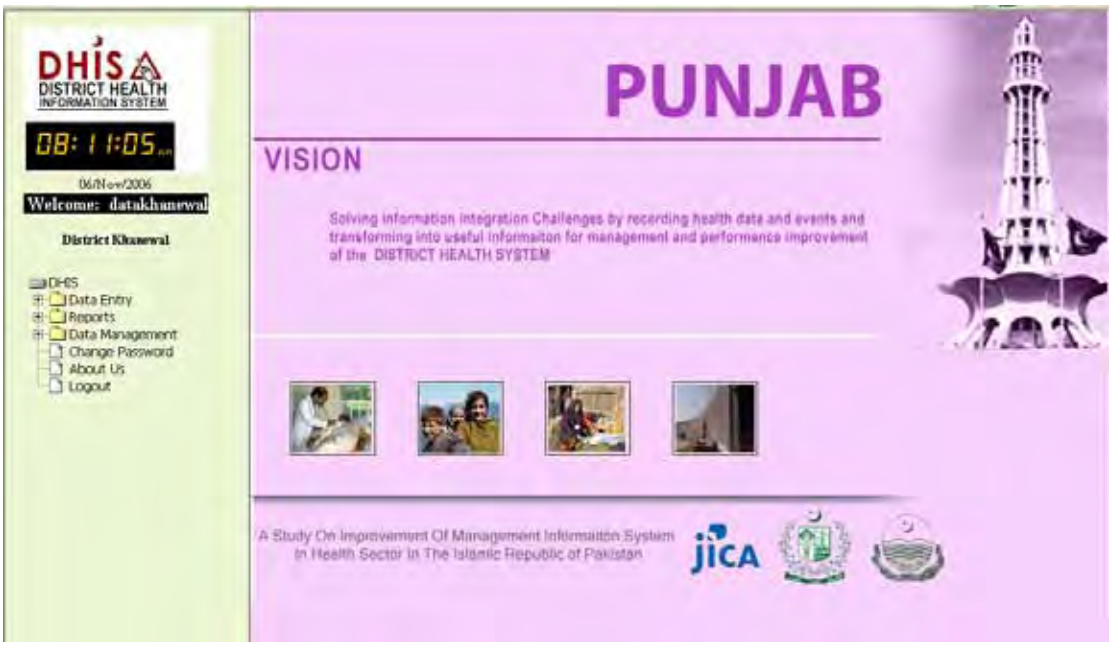


Figure: Sample Main Menu Screen

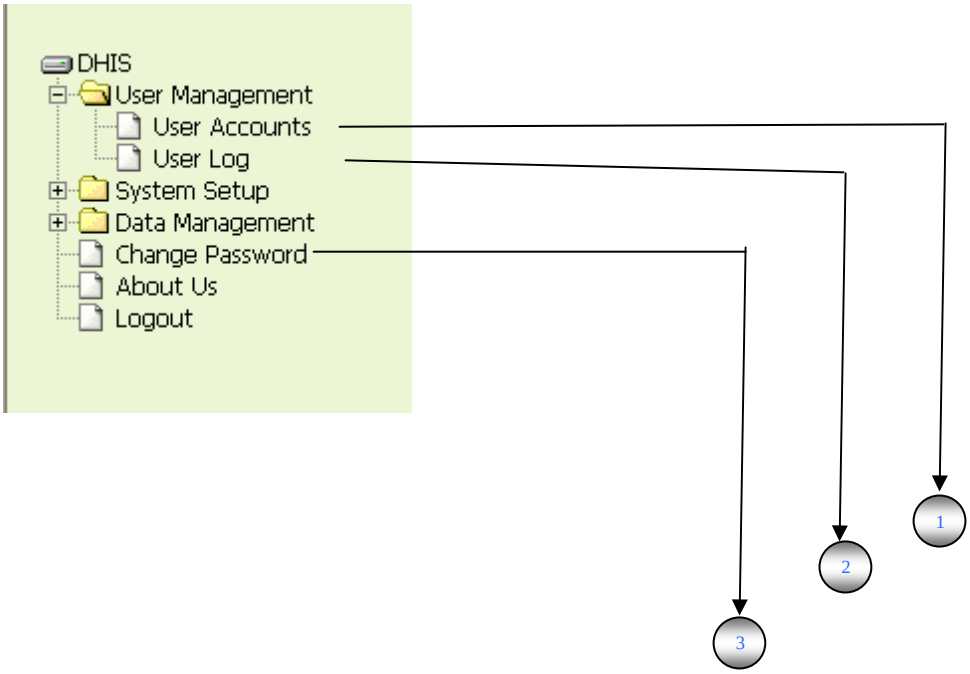
User management option can only be used by Administrator and this option will not appear in the menu of other regular users. Each user have rights to change his/her password.

Chapter – 3

User Management

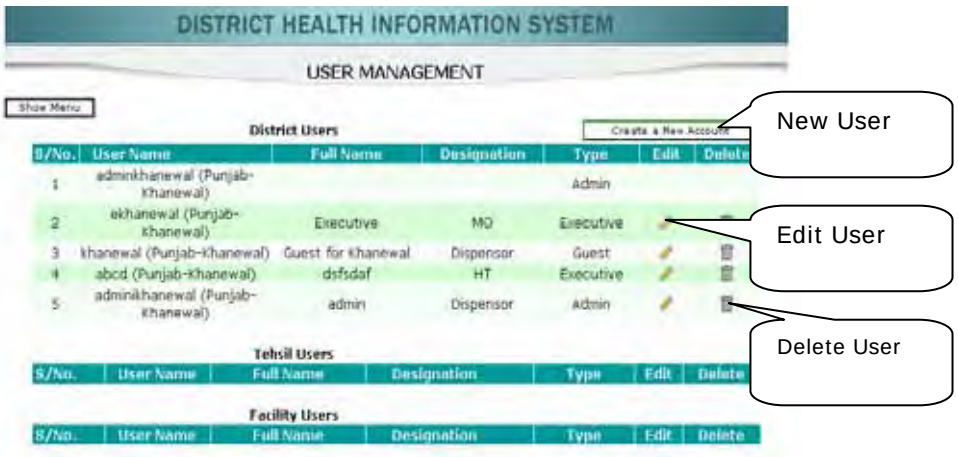
Details of User Management

This menu is enabled only to the 'Administrator' who has the privileges to create new Users/Administrators or to Edit or Delete them.



User Accounts

User Account menu is used to create new user, edit existing users and show list of existing users in the system, system generated S/No is assigned to every new user and his role (User Type) can be assign as Admin, Data Manager, executive or Guest (synchronization)



TO CREATE A NEW USER

1. To add a new user, click the *New* button following screen will appear.

2. Enter the user Login ID, User Password, User Type (Normal/Executive), Province and Facility in their respective fields.
3. Save the particulars by clicking the *Save* button. The moment you press the save button, the system generates a S/No and Save Users.

TO DELETE A USER

4. To delete a user, press the *Delete* button followed to User record. This action will also delete all the privileges assigned to that user.

Note No one is allowed to Edit, Delete or Change Password of the Master Administrator.

TO EDIT A USER RECORD

To Edit a record, click the *Edit* button followed to User record. Make the desired changes and click the *Save* button to save user.

User Rights

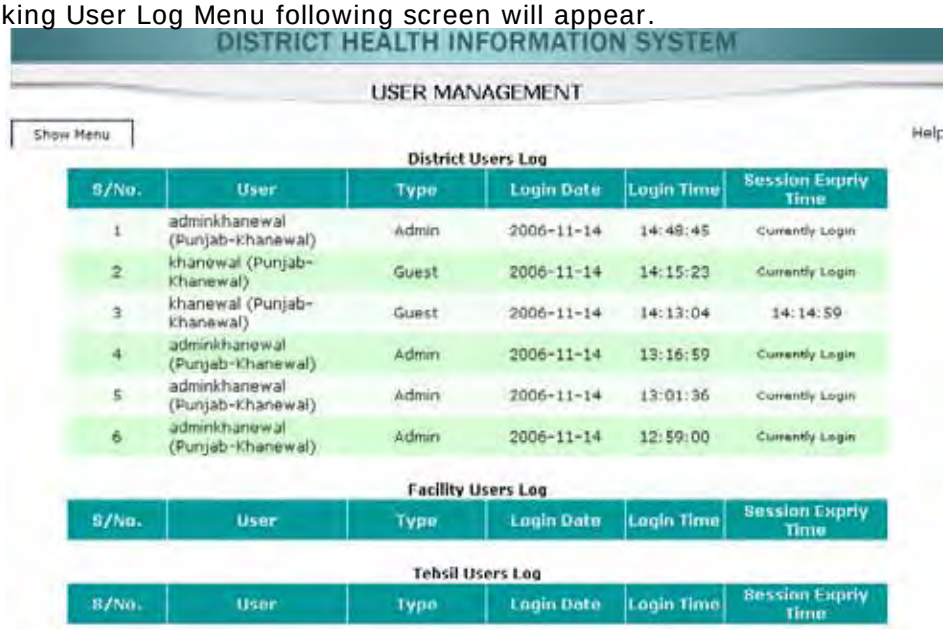
User type option is available to only system administrator and used to define the user role and assign different user rights to existing users. Administrator can set the role for users to manage different operations such as Data Entry, Data Management, Reports, User Management, System setups, and executive and guests users.

By selecting user type rights will show at right side of screen. User can be an Admin, Data manager, executive or guest for lower level.

User Type	Privileges
Admin	• User Management • System Setups
Data Manager (Applicable on District)	• Data Entry • Data Management • Reports
Executive	• Executive Dashboard • Reports
Guest	• Data synchronization (for lower level)

User Log

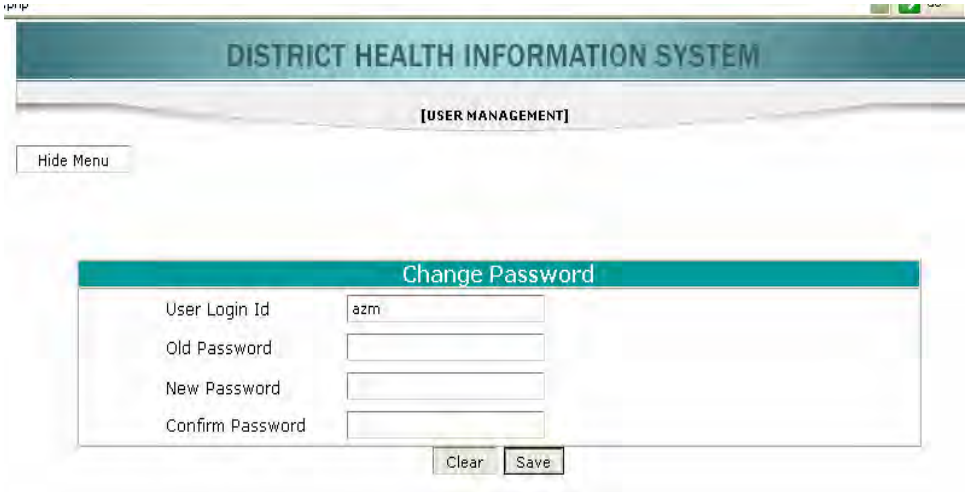
By Clicking User Log Menu following screen will appear.



This screen show the detail log of users who are currently logged in.

Changing Password

By Clicking change password menu following screen will appear.



1. Show the Name of User.
2. Type the old password.
3. Type New Password.
4. Confirm password.
5. Press Save button to save changes.
6. Press Clear button to Rest changes.

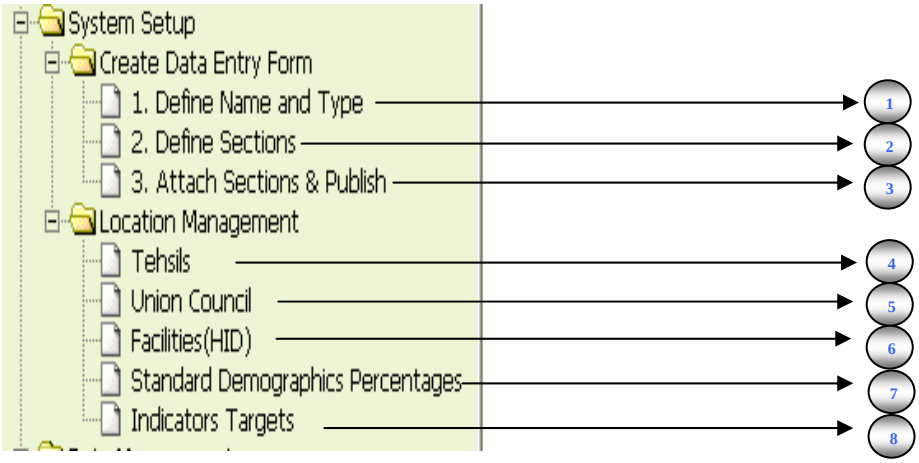
Chapter – 4

DHIS System Setup

System Setups (Level Wise)

User will see the screen of system setup as per his level and user rights; mainly system setup is divided in following levels.

Create data Entry form		**Applicable Level**
	Define Name and Type	Federal, Province, District
	Define Sections	Federal, Province, District
	Attach Sections & Publish	Federal, Province, District
Location Management		
	Designation	Federal
	Facility Type	Federal
	Province	Federal
	District	Province
	Tehsil	Province, District
	Union Council	Province, District
	Facilities (HID)	Federal, Province, District
	Standard Demographics Percentages	Federal, Province, District
	Indicators Targets	Federal, Province, District



Above screen shoot shows the menu which will appear in front of you.

Details of standard Functionalities

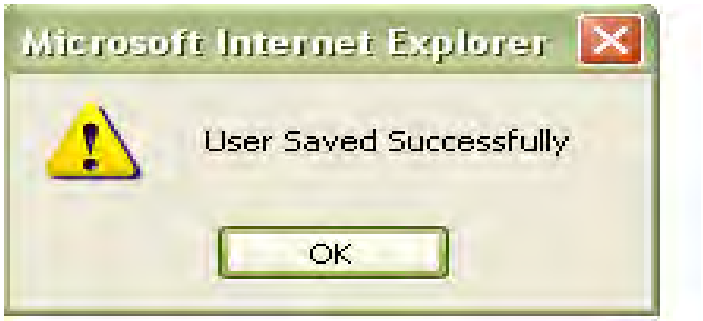
The monthly reporting application provides user following short cut keys for the software operation.

Icon	Description
*	Mandatory Field
Hide Menu	Hide Menu
Show Menu	Show Menu
Add New	Add a New Record
	Edit a Existing Record
Save	Save a Record
Clear	Clear an Entry
	Delete a Record
Back	Back to Previous Page
List	Show Existing Records
Preview	Preview Report
Rest	Reset Criteria
Export	Export Database
Import	Import Saved Database
Next>>	Next page
<<Previous	Previous Page

Details of Standard Messages

Save Changes

When click save button the following screen will appear:



By clicking *Ok* will be saved and move back to the existing records.

Duplicate Value

When some important value is duplicated (which should be unique in that particular screen) the following screen will appear:

By clicking *OK* the Duplicate Value message box will be closed and main form (on which working was in progress) will be activated again. Enter the unique value, otherwise box will appear again.

Delete Record

When click the *delete button* the following screen will appear:

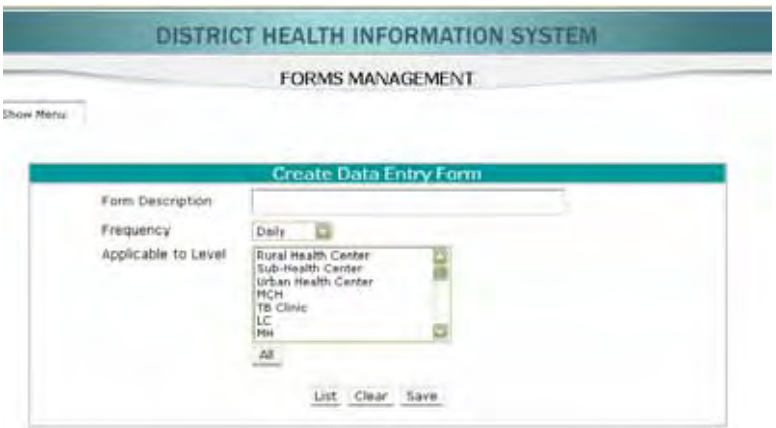
By clicking *Yes* the selected record will be permanently deleted and if click *No* the Delete Record message box will be closed and main list (on which working was in progress) will be activated again.

Define Name and Type.

When you will click on the ***Define Name and Type*** in the menu, following screen will appear in front of you

Enter New Record.

By Pressing New button following screen will appear in front of you.



1. **Form Description:** Enter the Name of Form.

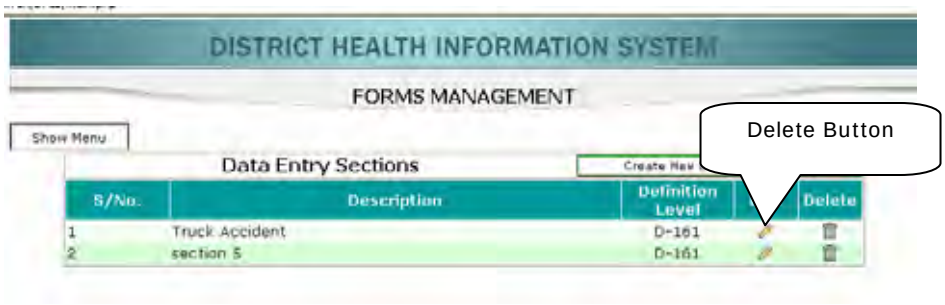
2. **Frequency:** Select Frequency(Monthly, Quarterly, yearly etc)
3. **Applicable Level:** Select Applicable Level (Rural Health Center etc). One or more level can be select at a time.
4. Press and hold control button and select one or more applicable level from List.
5. Press Back button to move previous page.
6. Press List button to Show Existing forms list.
7. Press Clear button to clear All fields
8. Press Save button to Save Form.

Edit Existing Record

By pressing Edit button (followed by the existing record) following screen will appear in front of you.

When you will press Edit button mentioned in figure above, data will be available for editing or modifying. You can also use this option to enter or change any missing information. After completing modification press ***save*** button to make changes permanent. During the data entry you can cancel your changes any time by using clear button or press back button to move on previous page

Delete Record



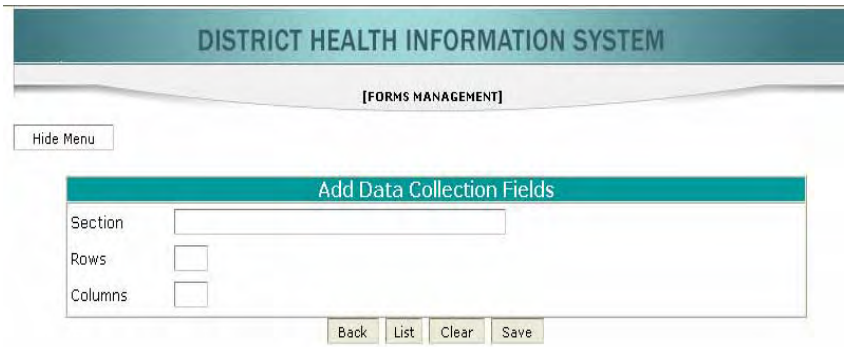
Press Delete button followed by existing record. When you press delete button it will ask for confirmation press Yes button to delete current record or No button to leave as it is.

Data Entry Sections

When you will click on the ***Data Entry Sections*** in the menu, following screen will appear in front of you

Enter New Record.

By Pressing New button following screen will appear in front of you.



1. **Section:** Enter the Name of Section (e.g Section I etc).
2. **Rows:** Specify Number of Rows for Section.
3. **Columns:** Specify Number of Columns for Section.
4. Press **Save** button to save record.
5. Press Back button to move previous page.

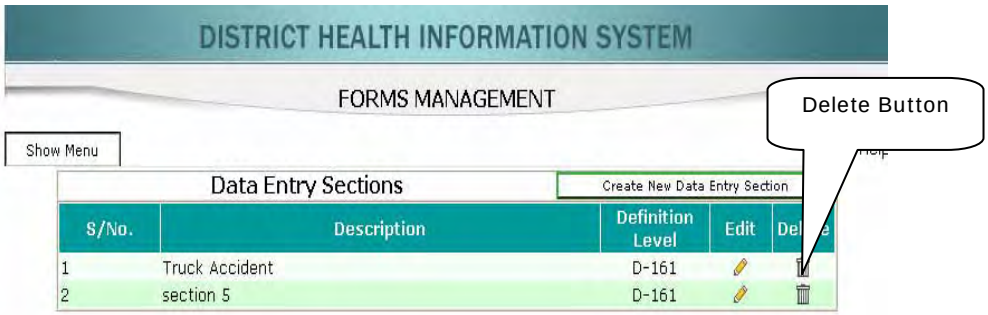
6. Press List button to Show Existing forms list.
7. Press Clear button to clear All fields

Edit Existing Record

By pressing Edit button (followed by the existing record) following screen will appear in front of you.

When you will press Edit button mentioned in figure above, data will be available for editing or modifying. You can also use this option to enter or change any missing information. After completing modification press ***save*** button to make changes permanent. During the data entry you can cancel your changes any time by using clear button or press back button to move on previous page

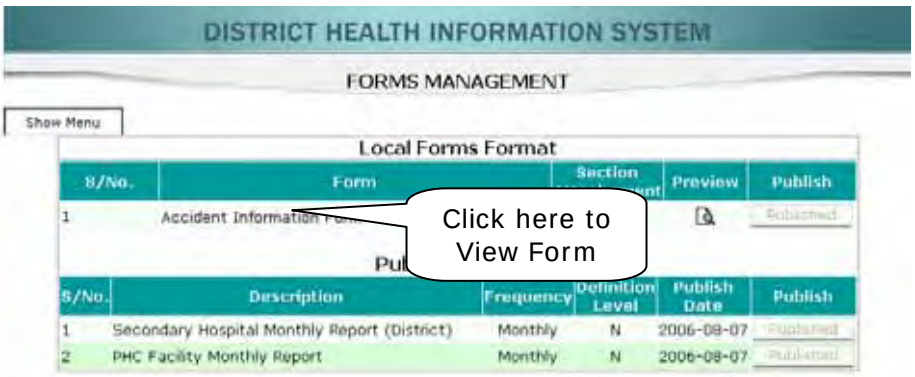
Delete Record



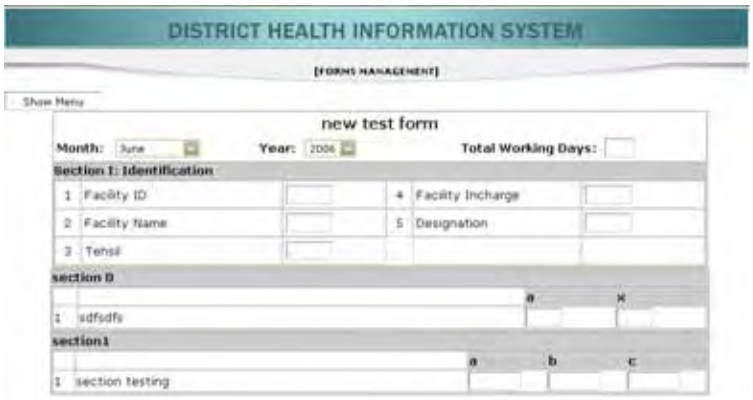
Press Delete button followed by existing record. When you press delete button it will ask for confirmation press Yes button to delete current record or No button to leave as it is.

Attach Sections and Publish.

When you will click on the ***Attach Sections and Publish*** in the menu, following screen will appear in front of you



Click on form to view Form sample. By Clicking on form following Screen will appear in front of you.

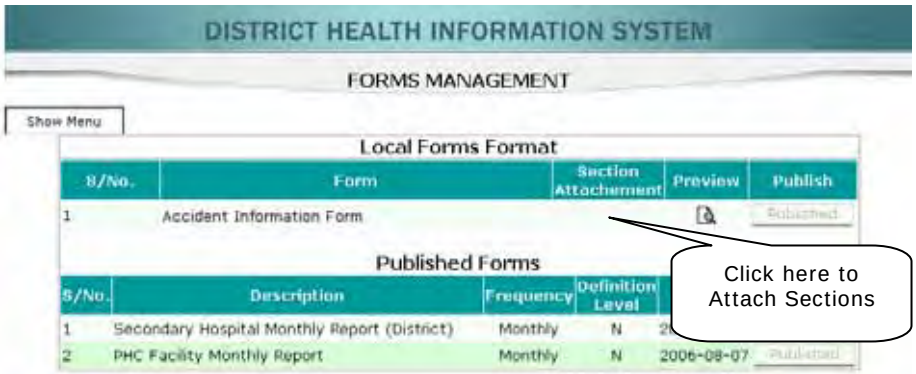


1. **Section I Identification:** This Section will show in all Forms as it is use to enter facility

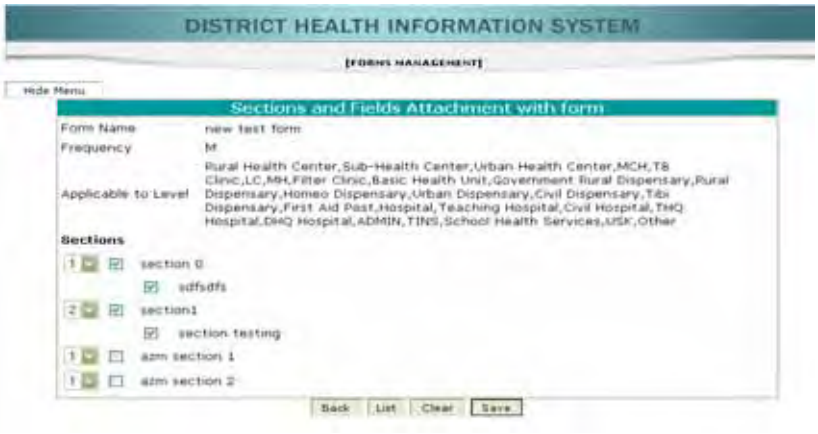
   data and reporting and Month/Year.

2. **Section II:** Rest of All Sections defines by user to use data entry.

Edit Existing Record

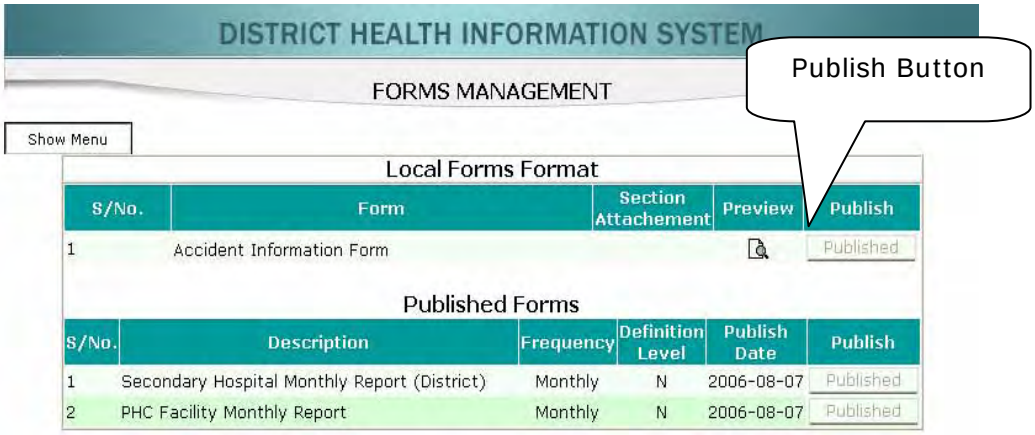


By pressing Section Attachment button (followed by the existing record) following screen will appear in front of you.



In this screen you can attached or detached the Section with. After completing modification press ***save*** button to make changes permanent. During the data entry you can cancel your changes any time by using clear button or press back button to move on previous page

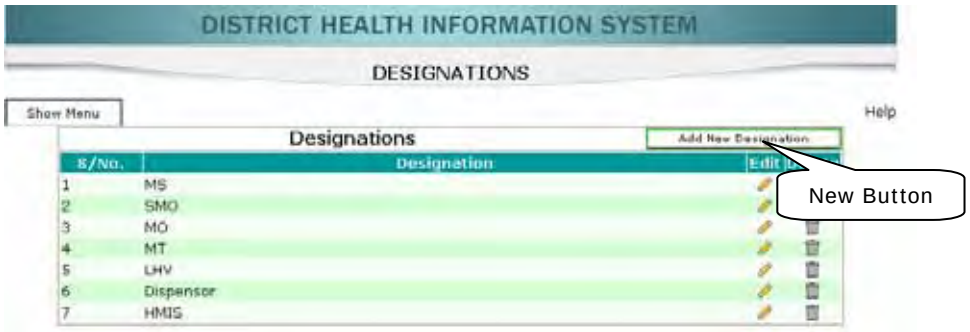
Publish Form



Press Publish button followed by existing record. When you press Publish button it will ask for confirmation press Yes button to publish current Form or No button to leave as it is. Once a form is published it will permanently saved and never be un-published. Un-published form can be edit or modify able.

Designation (Federal Level)

When you will click on the ***Designation*** in the menu, following screen will appear in front of you



Enter New Record

By Pressing New button following screen will appear in front of you.

Enter all required information and press save button to save Designation.

1. Enter the Designation
2. Press List button to Show Existing records.
3. Press Clear button to clear All fields
4. Press **Save** button to save data permanent.

Edit Existing Record

By pressing Edit button (followed by the existing record) following screen will appear in front of you.

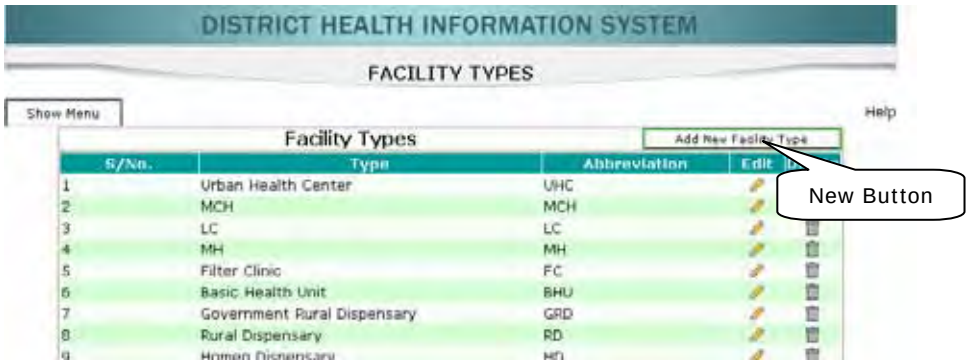
When you will press Edit button mentioned in figure above, data will be available for editing or modifying. You can also use this option to enter or change any missing information. After completing modification press ***save*** button to make changes permanent. During the data entry you can cancel your changes any time by using clear button or press back button to move on previous page

Delete Record

Press Delete button followed by existing record. When you press delete button it will ask for confirmation press Yes button to delete current record or No button to leave as it is.

Facility Type (Federal Level).

When you will click on the ***Facility Type*** in the menu, following screen will appear in front of you;



Enter New Record

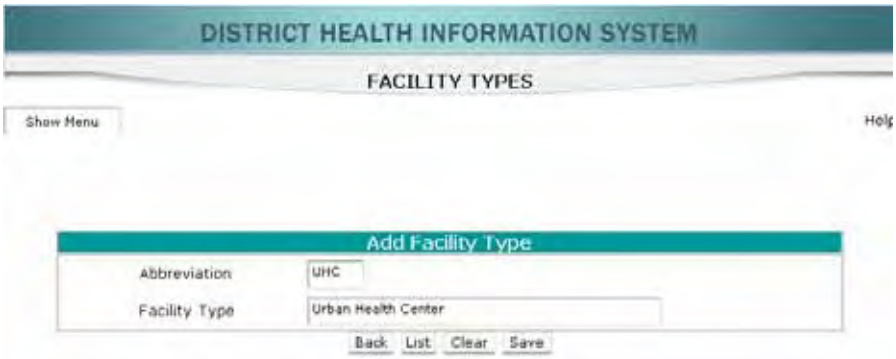
By Pressing New button following screen will appear in front of you.

Enter all required information and press save button to save Facility Type.

1. Enter the Facility Type Code
2. Enter the Name of Facility Type.
3. Target: Tick the target option where type will appear in target screen.
4. Press List button to Show Existing records.
5. Press Clear button to clear All fields
6. Press **Save** button to save data permanent.

Edit Existing Record

By pressing Edit button (followed by the existing record) following screen will appear in front of you.



When you will press Edit button mentioned in figure above, data will be available for editing or modifying. You can also use this option to enter or change any missing information. After completing modification press ***save*** button to make changes permanent. During the data entry you can cancel your changes any time by using clear button or press back button to move on previous page

Delete Record

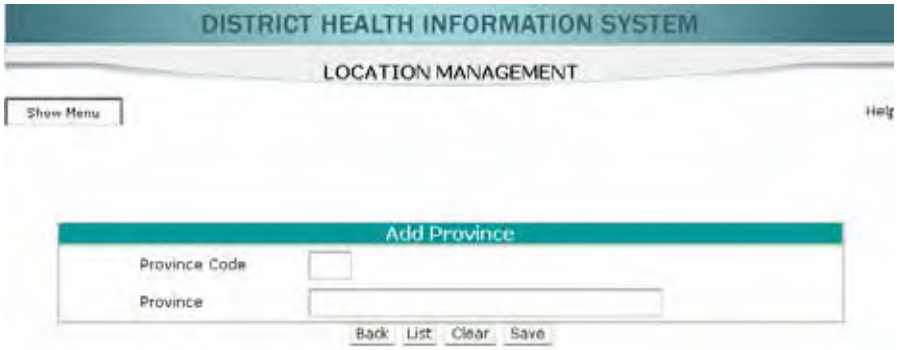
Press Delete button followed by existing record. When you press delete button it will ask for confirmation press Yes button to delete current record or No button to leave as it is.

Province (For Federal Level User)

When you will click on the ***Province*** in the menu, following screen will appear in front of you

Enter New Record

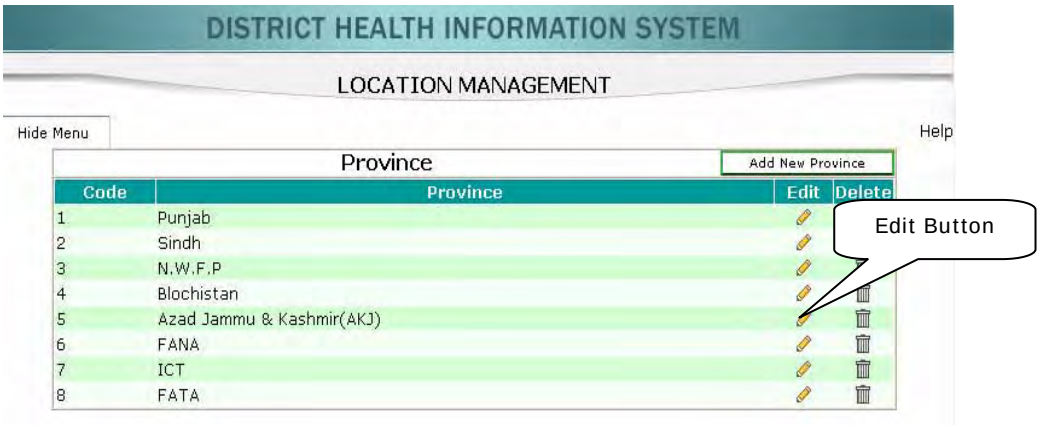
By Pressing New button following screen will appear in front of you.



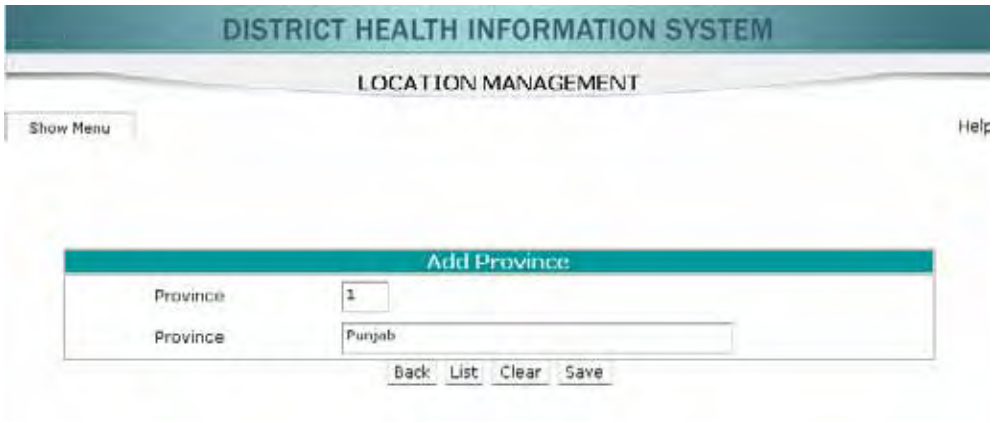
Enter all required information and press save button to save Province.

7. Enter the Province Code
8. Enter the Name of Province
9. Press List button to Show Existing records.
10. Press Clear button to clear All fields
11. Press **Save** button to save data permanent.

Edit Existing Record

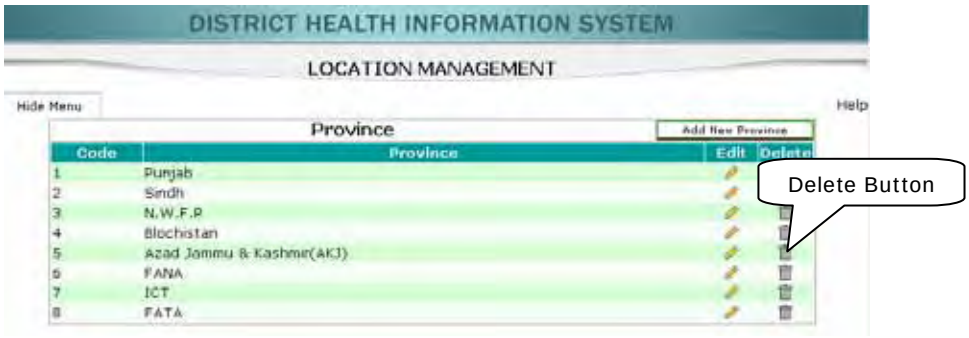


By pressing Edit button (followed by the existing record) following screen will appear in front of you.



When you will press Edit button mentioned in figure above, data will be available for editing or modifying. You can also use this option to enter or change any missing information. After completing modification press ***save*** button to make changes permanent. During the data entry you can cancel your changes any time by using clear button or press back button to move on previous page.

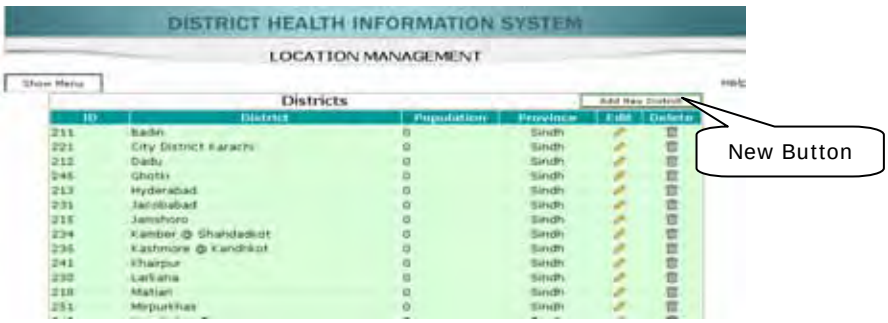
Delete Record



Press Delete button followed by existing record. When you press delete button it will ask for confirmation press Yes button to delete current record or No button to leave as it is.

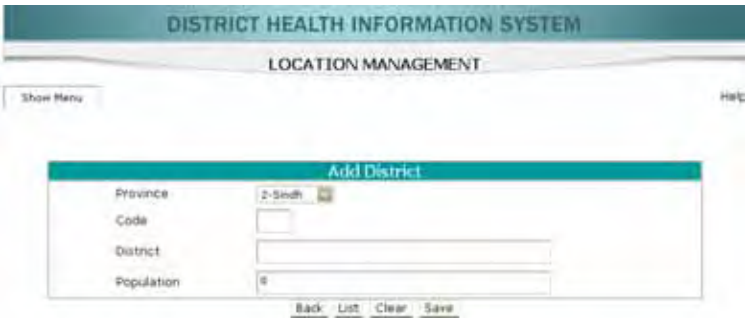
Districts (For Province Level User)

When you will click on the ***Districts*** in the menu, following screen will appear in front of you



Enter New Record

By Pressing New button following screen will appear in front of you.

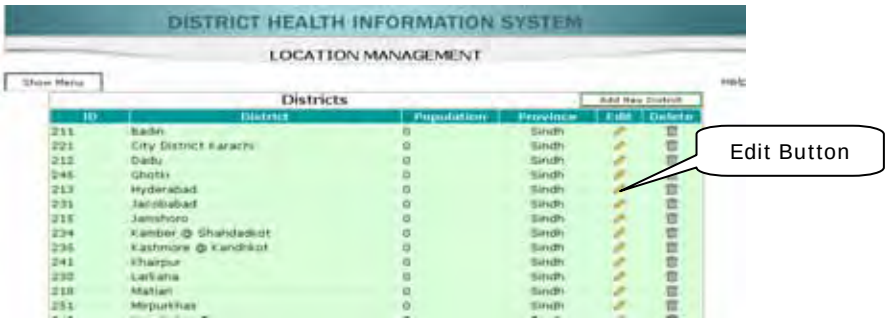


Enter all required information and press save button to save District.

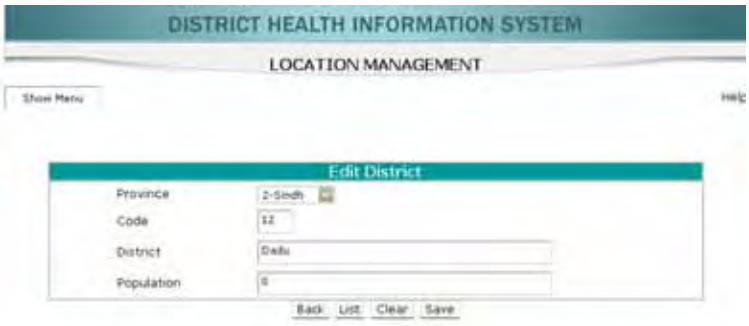
1. Select Province from List
2. Enter district code, name and population.
3. Press Back button to move previous page.
4. Press List button to Show Existing records.

5. Press Clear button to clear All fields
6. Press **Save** button to save data permanent.

Edit Existing Record

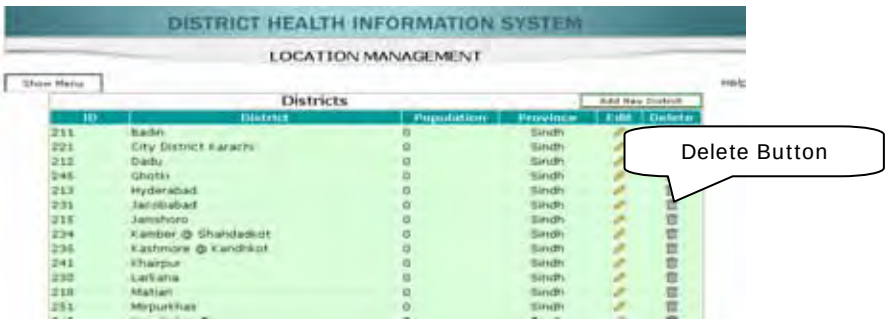


By pressing Edit button (followed by the existing record) following screen will appear in front of you.



When you will press Edit button mentioned in figure above, data will be available for editing or modifying. You can also use this option to enter or change any missing information. After completing modification press ***save*** button to make changes permanent. During the data entry you can cancel your changes any time by using clear button or press back button to move on previous page

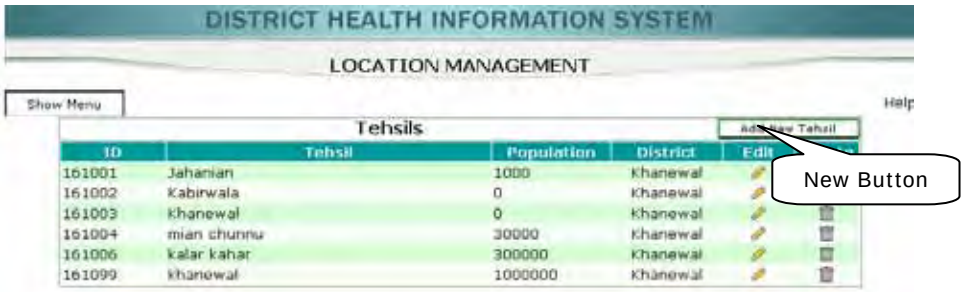
Delete Record



Press Delete button followed by existing record. When you press delete button it will ask for confirmation press Yes button to delete current record or No button to leave as it is.

Tehsil (Province and District Users)

When you will click on the ***Tehsil*** in the menu, following screen will appear in front of you



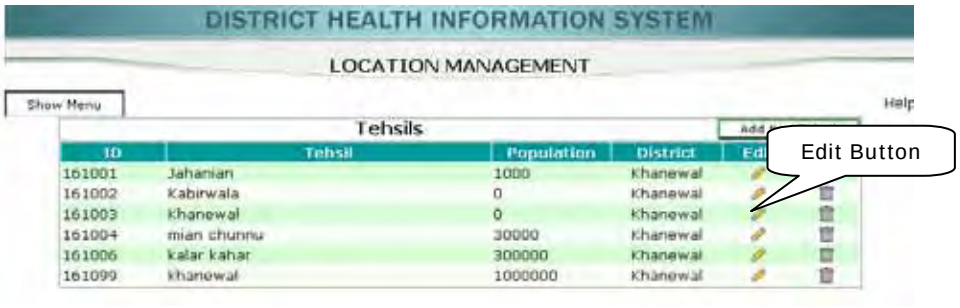
Enter New Record.

By Pressing New button following screen will appear in front of you.

Enter all required information and press save button to save tehsil.

1. Select Province from List
2. Select District from List
3. Enter tehsil code, name and population.
4. Press Back button to move previous page.
5. Press List button to Show Existing records.
6. Press Clear button to clear All fields
7. Press **Save** button to save data permanent.

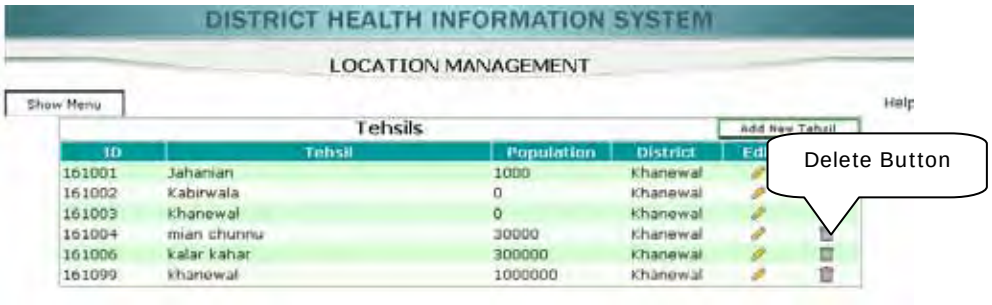
Edit Existing Record



By pressing Edit button (followed by the existing record) following screen will appear in front of you.

When you will press Edit button mentioned in figure above, data will be available for editing or modifying. You can also use this option to enter or change any missing information. After completing modification press ***save*** button to make changes permanent. During the data entry you can cancel your changes any time by using clear button or press back button to move on previous page

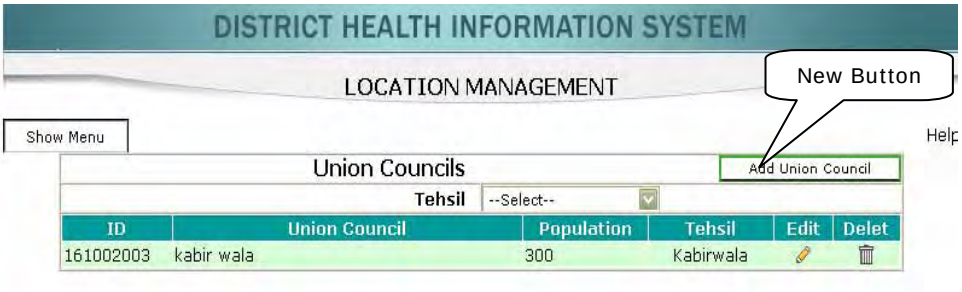
Delete Record



Press Delete button followed by existing record. When you press delete button it will ask for confirmation press Yes button to delete current record or No button to leave as it is.

Union Council (For Province, District Level User)

When you will click on the ***Union Council*** in the menu, following screen will appear in front of you



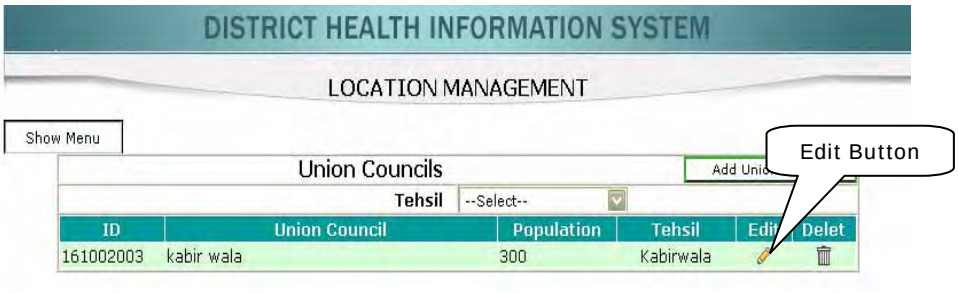
Enter New Record

By Pressing New button following screen will appear in front of you.

Enter all required information and press save button to save data.

1. Select Province from List.
2. Select District from List.
3. Select Tehsil from List.
4. Enter Union Council Code, name and population.
5. Press Back button to move previous page.
6. Press List button to Show Existing records.
7. Press Clear button to clear All fields
8. Press Save button to save data permanent.

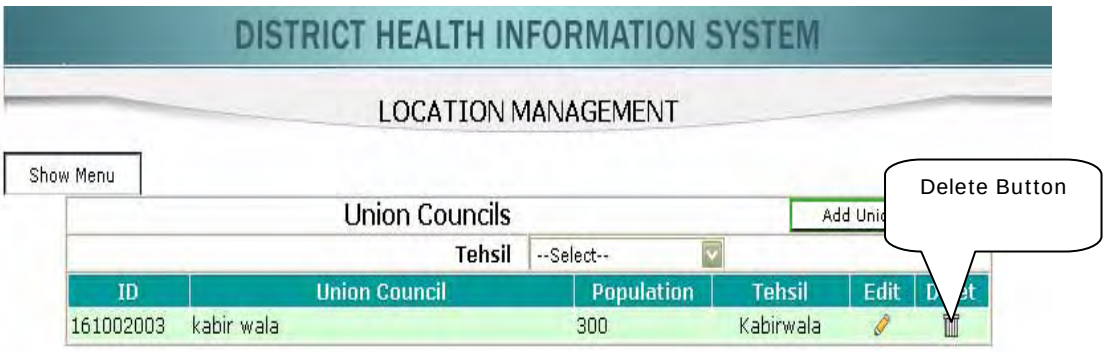
Edit Existing Record



By pressing Edit button (followed by the existing record) following screen will appear in front of you.

When you will press Edit button mentioned in figure above, data will be available for editing or modifying. You can also use this option to enter or change any missing information. After completing modification press ***save*** button to make changes permanent. During the data entry you can cancel your changes any time by using clear button or press back button to move on previous page

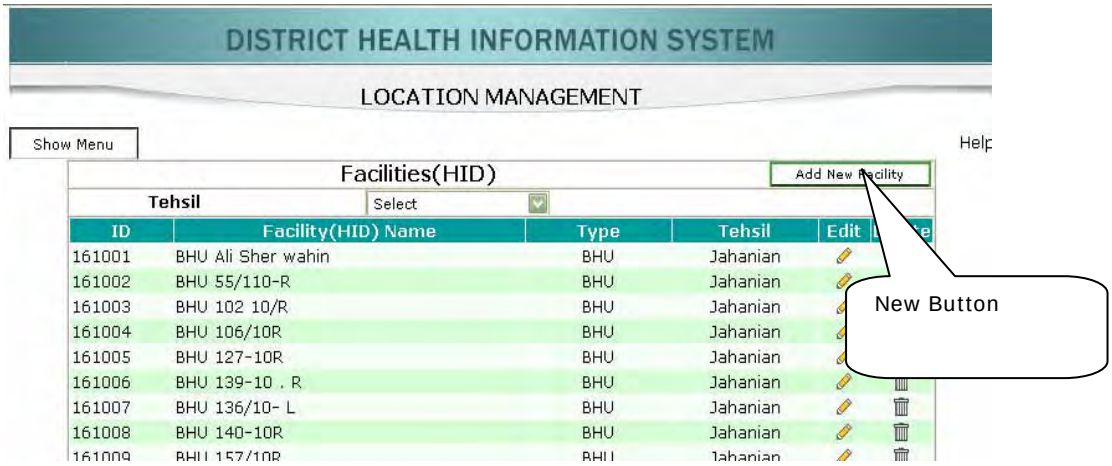
Delete Record



Press Delete button followed by existing record. When you press delete button it will ask for confirmation press Yes button to delete current record or No button to leave as it is.

Facilities (HID) (For Federal, Province, District Level User)

When you will click on the ***Facilities (HID)*** in the menu, following screen will appear in front of you

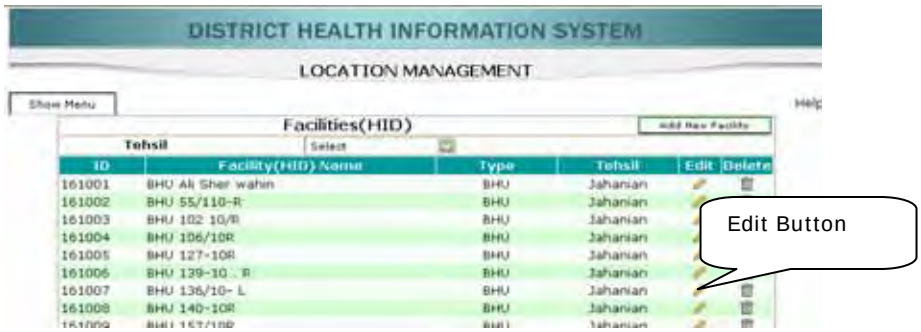


Enter New Record.

By Pressing New button following screen will appear in front of you.

1. **Province** Select Province from List.
2. **District** Select District from list. It will show the districts under selected province.
3. **Tehsil**: Select Tehsil from tehsil list. It will show the tehsil under selected district.
4. **Union Council:** Select union council from list. It will show union councils under selected tehsil.
5. **Code:** Enter Facility Code
6. **Facility Name:** enter the Name of Facility.
7. **Facility Type:** Select Facility Type from List.
8. **Area Type:** Select Area Type from List.
9. **Incharge:** Enter Incharge name.
10. **Designation:** Select Incharge Designation.
11. **Catchments Area POP:** Enter the Facility catchments area population.
12. **Class:** Select the Class from List.
13. **Functional Status:** Select the status of facility from list.
14. **Reporting Status:** Select the facility reporting status.
15. Press List button to Show Existing forms list.
16. Press Clear button to clear All fields
17. Press Save button to save data.

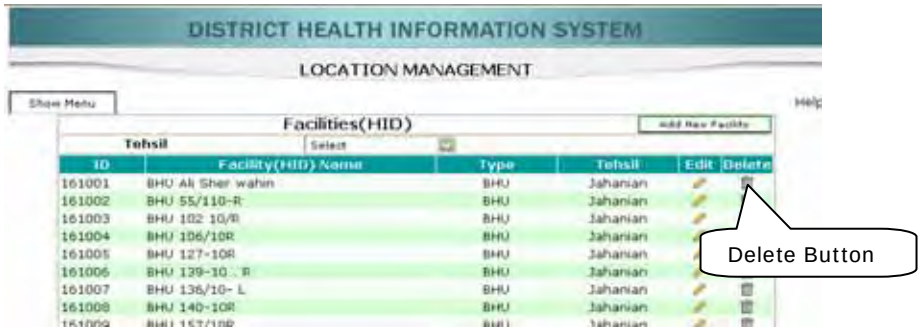
Edit Existing Record



By pressing Edit button (followed by the existing record) following screen will appear in front of you.

When you will press Edit button mentioned in figure above, data will be available for editing or modifying. You can also use this option to enter or change any missing information. After completing modification press ***save*** button to make changes permanent. During the data entry you can cancel your changes any time by using clear button or press back button to move on previous page

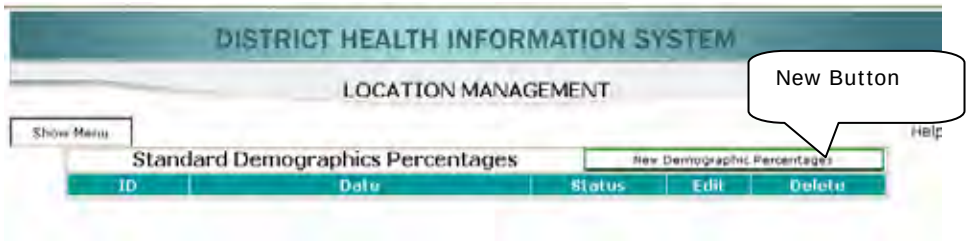
Delete Record



Press Delete button followed by existing record. When you press delete button it will ask for confirmation press Yes button to delete current record or No button to leave as it is.

Standard Demographic Percentages

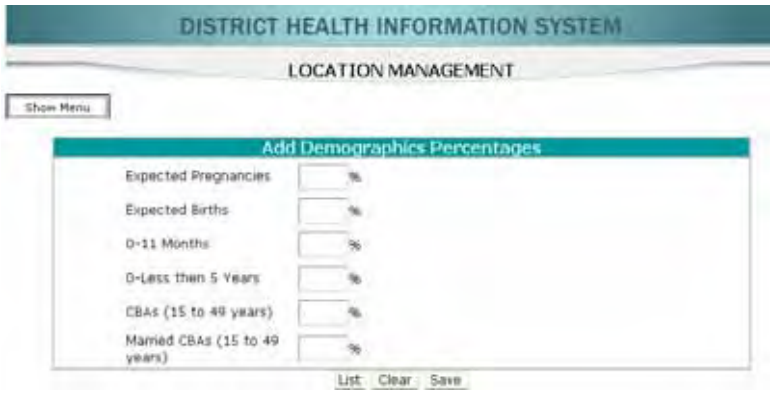
When you will click on the ***Standard Demographic percentages*** in the menu, following screen will appear in front of you



These percentages will help to generate indicator based reports it is necessary to enter first time. User can modify values and also can active or in-active if more then one percentage enters.

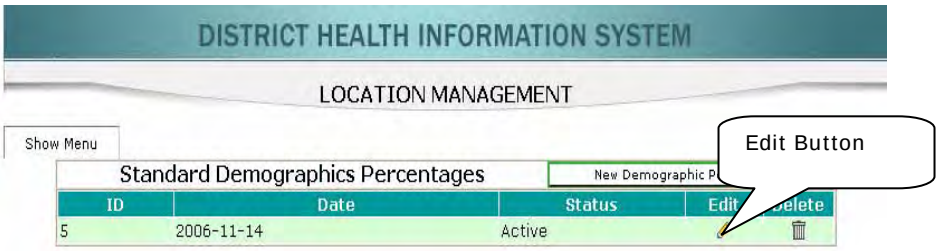
Enter New Record

By Pressing New button following screen will appear in front of you.



1. Enter the Percentages.
2. Press List button to Show Existing data.
3. Press Clear button to clear All fields
4. Press Save button to save data.

Edit Existing Record

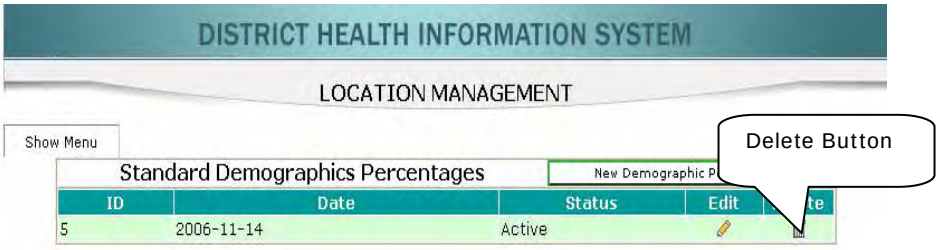


By pressing Edit button (followed by the existing record) following screen will appear in front of you.

When you will press Edit button mentioned in figure above, data will be available for editing or modifying. You can also use this option to enter or change any missing information. After completing modification press ***save*** button to make changes permanent.
During the data entry you can cancel your changes any time by using clear button or press back button to move on previous page

Note: User cans active or in-active current percentages.

Delete Record



Press Delete button followed by existing record. When you press delete button it will ask for confirmation press Yes button to delete current record or No button to leave as it is.

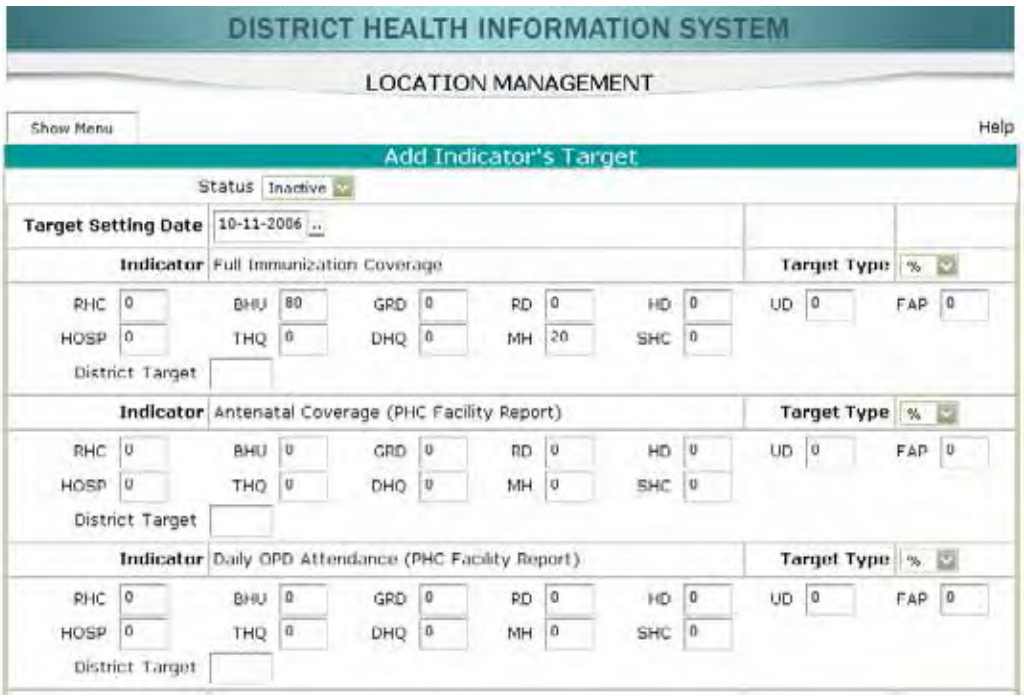
Indicator Targets

When you will click on the ***Indicator Targets*** in the menu, following screen will appear in front of you

These indicators will draw a line in reports to show facilities above and bellow the targets. User can modify values and also can active or in-active if more then one indicator targets enter.

Enter New Record.

By Pressing New button following screen will appear in front of you.



1. Select the indicator target either in Percentage or Number.
2. Enter the target type wise.
3. Targets will show on reports
4. Press List button to Show Existing data.
5. Press Clear button to clear All fields
6. Press Save button to save data.

Note: Only Those facility types will be shown on target screen which were ticked on facility type screen.

Edit Existing Record

By pressing Edit button (followed by the existing record) following screen will appear in front of you.

When you will press Edit button mentioned in figure above, data will be available for editing or modifying. You can also use this option to enter or change any missing information. After completing modification press ***save*** button to make changes permanent. During the data entry you can cancel your changes any time by using clear button or press back button to move on previous page.

Note: User can active or in-active current Targets.

Delete Record

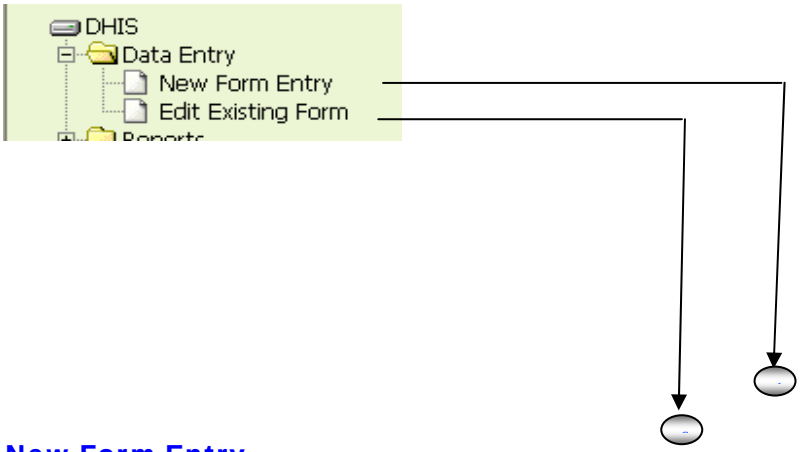
Press Delete button followed by existing record. When you press delete button it will ask for confirmation press Yes button to delete current record or No button to leave as it is.

Chapter -5

Monthly Form Data Entry

Monthly Forms Data Entry (District Level)

The user with the rights of data entry can access this option in the DHIS software, and can add new monthly report or edit existing monthly report.

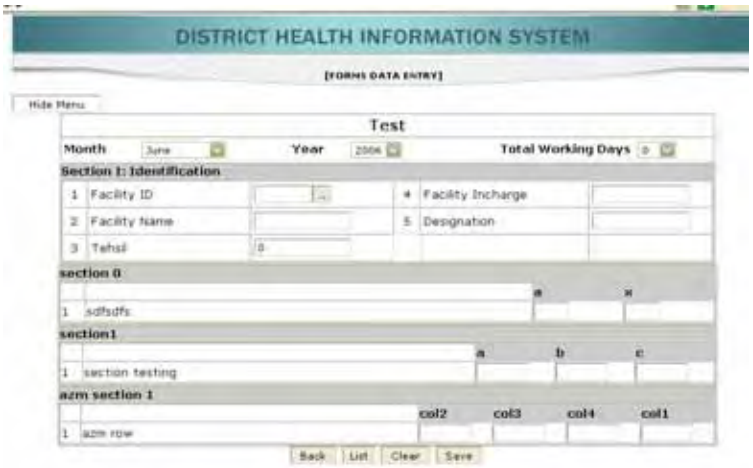


New Form Entry

When you will click on the ***New Form Entry*** in the menu, following screen will appear in front of you

Enter New Record.

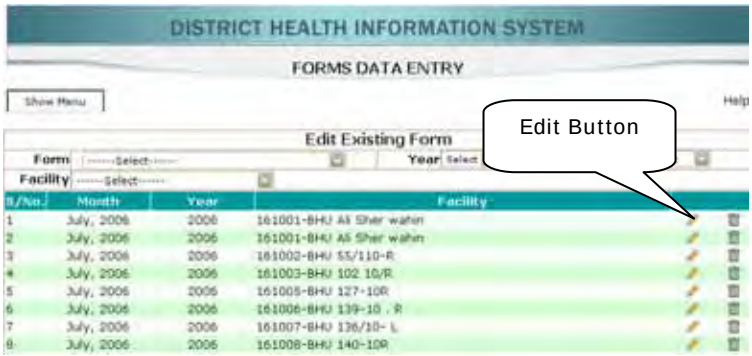
By Pressing New button following screen will appear in front of you.



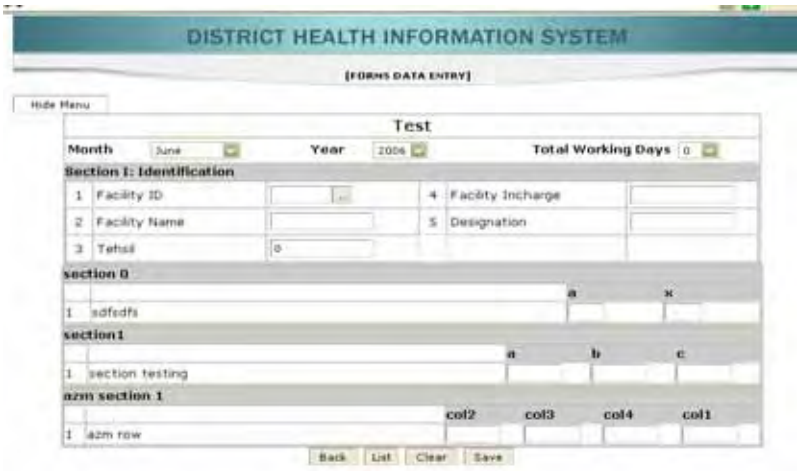
Select facility ID from list some of fields automatically fill by selecting facility (e.g Facility name, Incharge etc) and rest of fields and section available for data entry. Now start entering data after completion of data press save button to save data.

Edit Existing Form

When you will click on the ***Edit Existing Form*** in the menu, following screen will appear in front of you

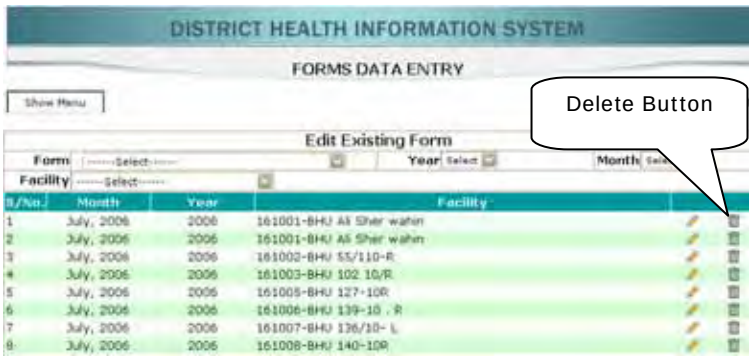


Different search filters are available to search a particular form or can select from list under the search filters. By pressing Edit button (followed by the existing record) following screen will appear in front of you.



When you will press Edit button mentioned in figure above, data will be available for editing or modifying. You can also use this option to enter or change any missing information. After completing modification press ***save*** button to make changes permanent. During the data entry you can cancel your changes any time by using clear button or press back button to move on previous page

Delete Record



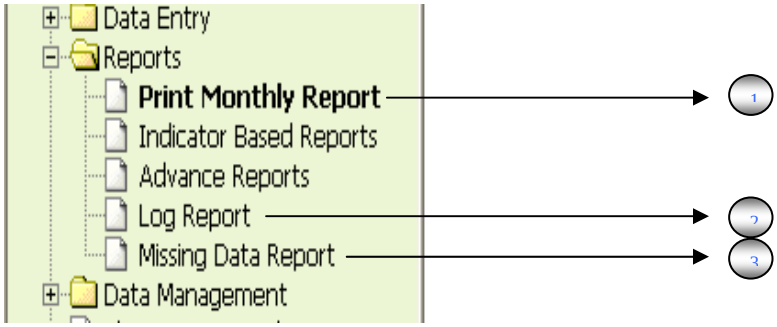
Press Delete button followed by existing record. When you press delete button it will ask for confirmation press Yes button to delete current record or No button to leave as it is.

Chapter - 6

Routine Reports

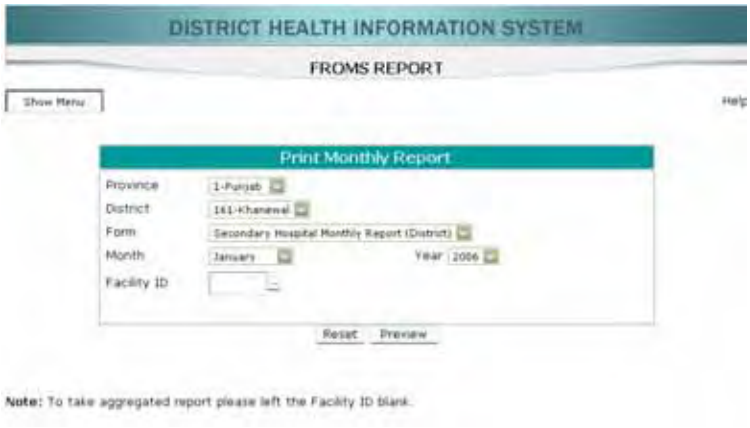
Routine Reports

The user with the rights of data entry can access this option in the DHIS software, and can generate monthly routine reports based on current or previous month data.



Print Monthly Report Form

When you will click on the ***Print Monthly Report From*** in menu, following screen will appear in front of you.



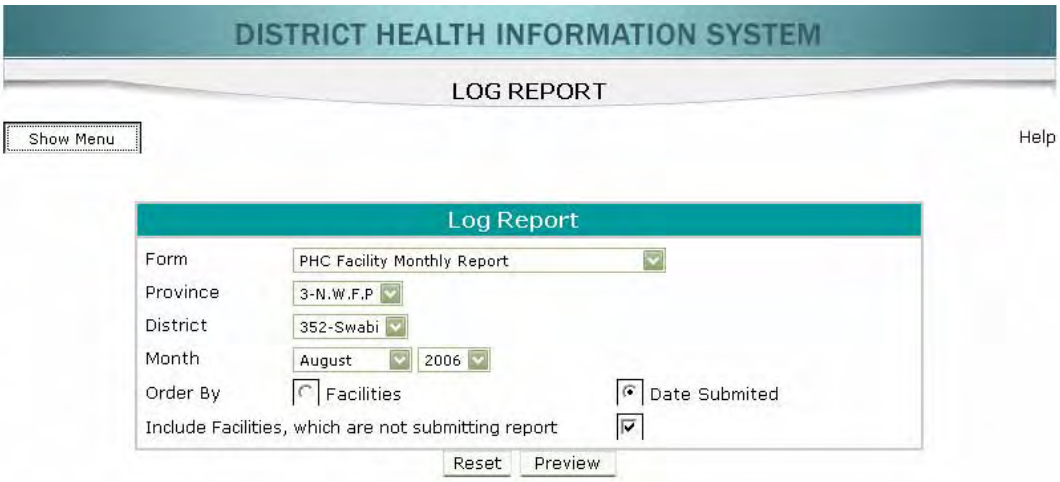
It will show the preview of data entry form with fill data and without any data.

Following Criteria can be apply on Report

- Province.
- District.
- Form type.
- Month
- Year
- Facility ID
- Press preview button to get preview of form
- Clear all fields by pressing reset button.
- To take aggregated report please left the Facility ID blank.

Log Report.

When you will click on the ***Log Report*** in menu, following screen will appear in front of you.



It will show the preview of monthly reports submitted or not submitted by facilities for selected month. Following Criteria can be apply on Report

- Form: Select Form type (PHC or Secondary hospital).
- Province: Select Province from List
- District: Select District From list
- Month: Specify the Month
- Year: Specify the year
- Order by Facilities: Will show the Report ascending order by facility ID.
- Data Submitted: Will show the Report ascending order by submission date.
- Tick to include facilities, which are not submitted report in specified month.
- Press preview button to get preview of form
- Clear all fields by pressing reset button.
- To take aggregated report please left the Facility ID blank.

Missing Data Report

When you will click on the ***Missing Data Report*** in menu, following screen will appear in front of you.

It will show the preview of blanks fields of monthly for the selected month. Following Criteria can be apply on Report

- Form: Select Form type (PHC or Secondary hospital).
- Province: Select Province from List
- District: Select District From list
- Month: Specify the Month
- Year: Specify the year
- Press preview button to get preview of form
- Clear all fields by pressing reset button.

Chapter – 7

Indicator Reports

Indicator based Report

When you will click on the ***indicator based report*** in menu, following screen will appear in front of you.

It will show the preview of selected indicator based report, Following Criteria can be apply on Report

- Report (Indicator)
- Province.
- District.
- Month
- Year
- Facility Type (BHU, RHC etc)
- Graph (Yes/No)
- Press preview button to get preview of form
- Clear all fields by pressing reset button.
- The reports are based on the Demographic Percentages

Chapter – 8

Advance Reports

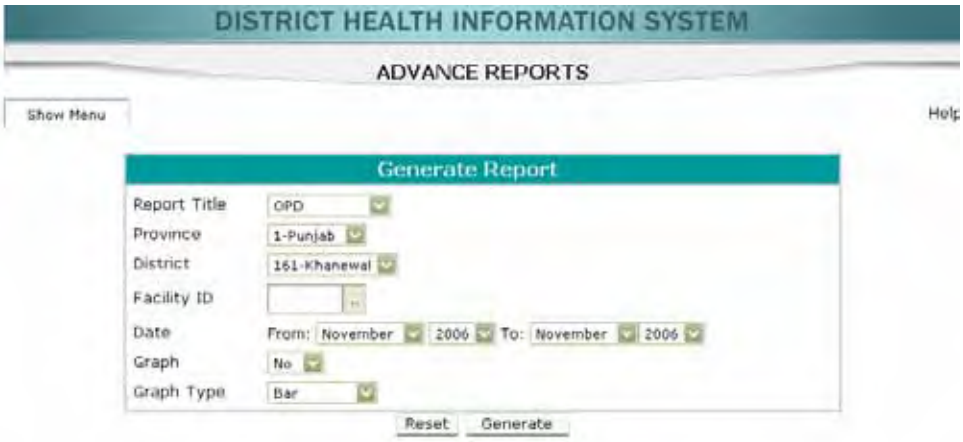
Advance Report.

When you will click on the ***Advance Report*** in menu, following screen will appear in front of you.

Click on the New link to create and new report. When you click on the new following screen will appear in front of you.

Type the name of report and select the section or data element of report. Once data element select its related field will in front of you select one or more fields from list and press save button to save report.

Now click on the newly develop or already developed report will show the following criteria screen.



Following Criteria can be apply on Report

- Report Title (Name of Advance Report)
- Province.
- District.
- Facility
- Date Range (From Month/year and To Month/year)
- Graph (Yes/No)
- Graph type (Bar/Correlation)
- Press preview button to get preview of report.

Clear all fields by pressing reset button.

Chapter – 9

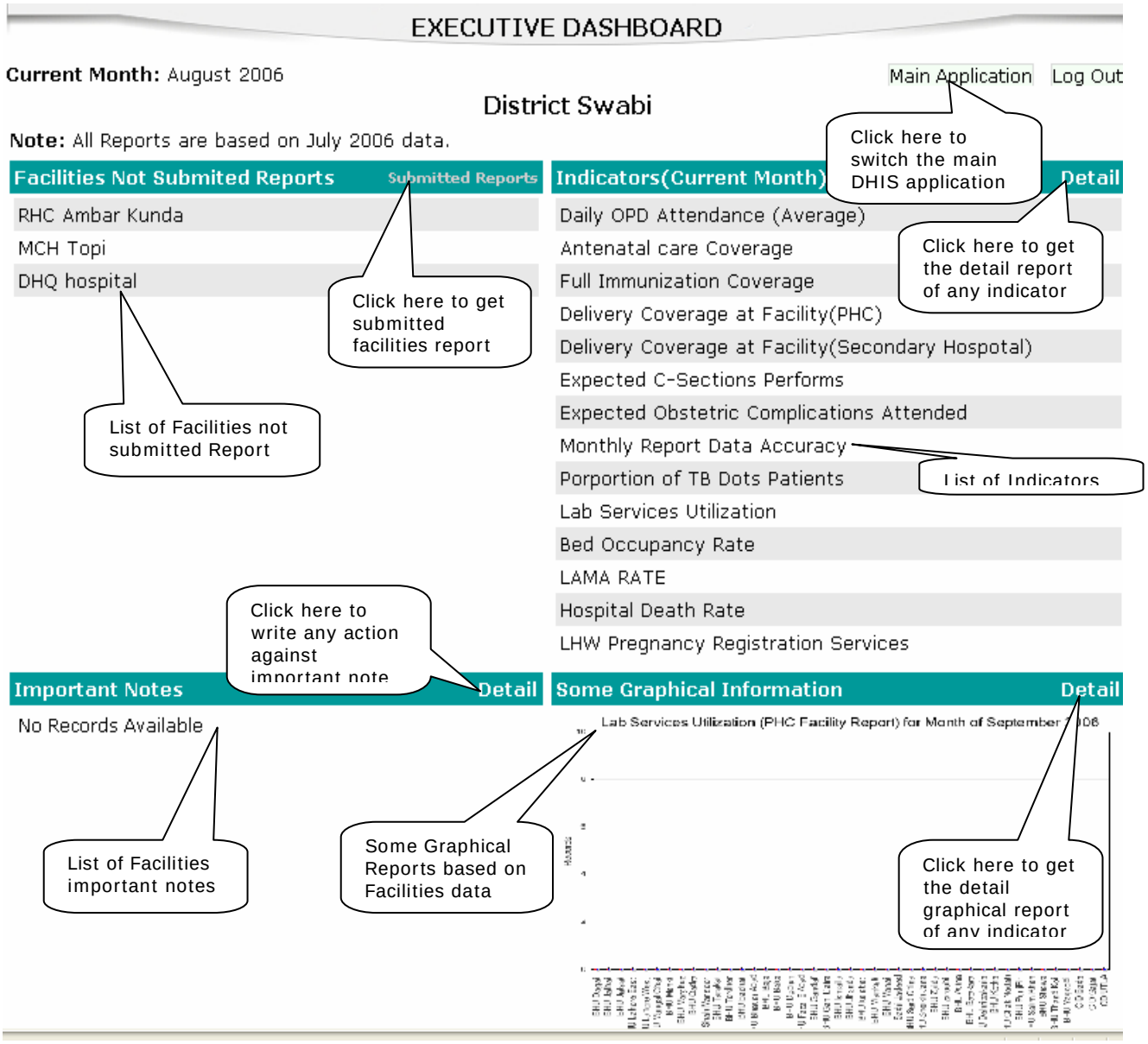
Executive Dashboard

Executive Dashboard

User can login with executive user type. This will show maximum information in single screen.

Following some important feathers of executive dashboard

- Main application: Click main application button to switch detail reporting section. User can view the detail list of report including indicator based and advance reports.
- Left Top side of screen: This will show the List of un-submitted reports. By clicking on submitted reports button to view list of facilities which reported submitted for previous month.
- Right Top side of screen: this will show some important indicator list by clicking on any indicator user will get single report of current month by facilities with graphical view. Click on the detail button to view detail of any indicator on the specified month and year.
- Left Bottom Side of screen: this will show the some important note submitted by facility. By clicking on detail button user can write action against any important note.
- Right bottom side of screen: some graphical view of indicators. By clicking on graph it will zoom the view of graph.

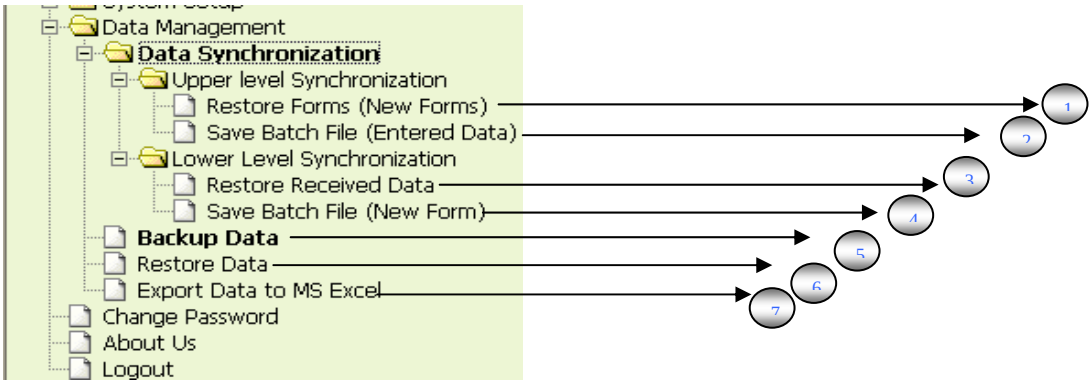


Chapter – 10

Data Synchronization

Data Management

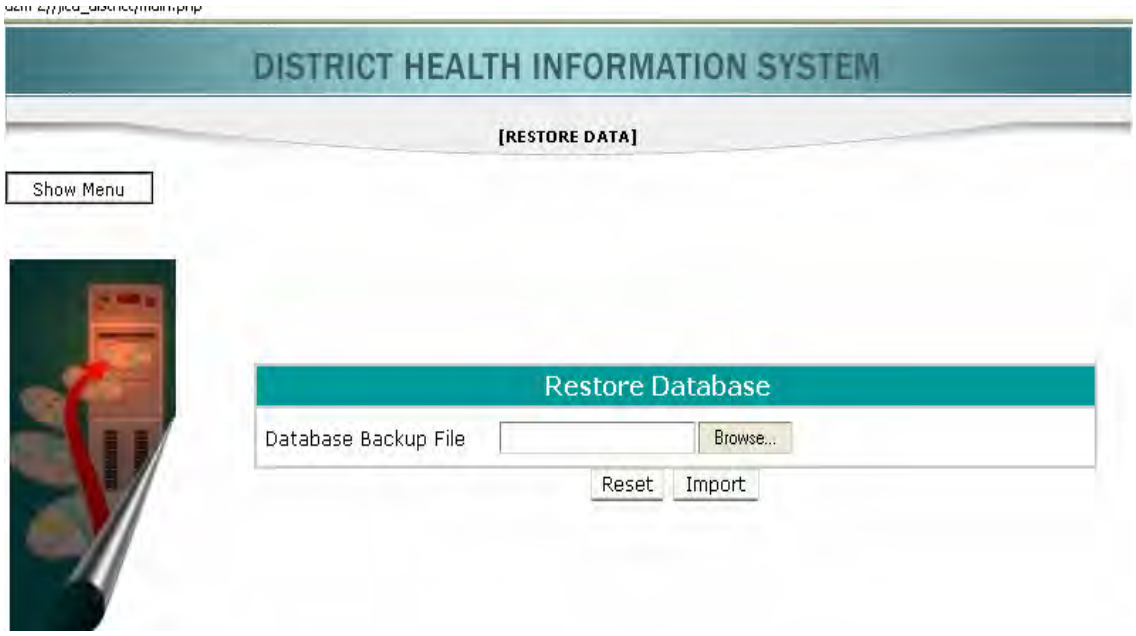
The user with the rights of data management can access this option in the DHIS software, and can use the synchronization process for data management.



Data Synchronization

Upward Synchronization

When you will click on the ***Restore Forms*** in upward Synchronization menu, following screen will appear in front of you.

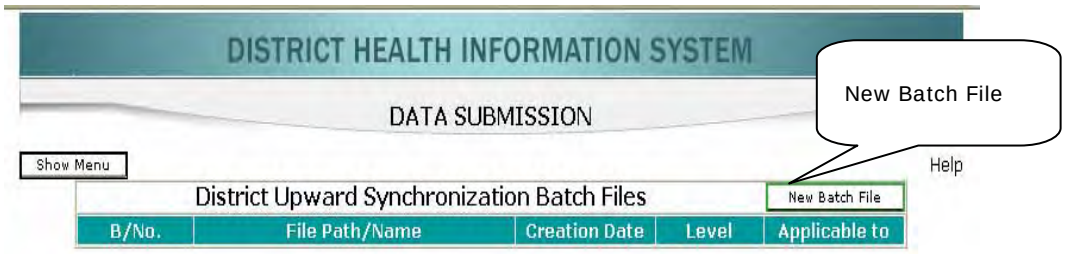


- Click browse button to select database dump file.
- Press import button to restore new data.
- Clear all fields by pressing reset button.

Note: This Screen will use when any update available in upper level. The can contain system setup information and any new form for data entry.

Save batch file (Entered Data).

When you will click on the ***Save batch file (Entered data)*** in upward Synchronization menu, following screen will appear in front of you.



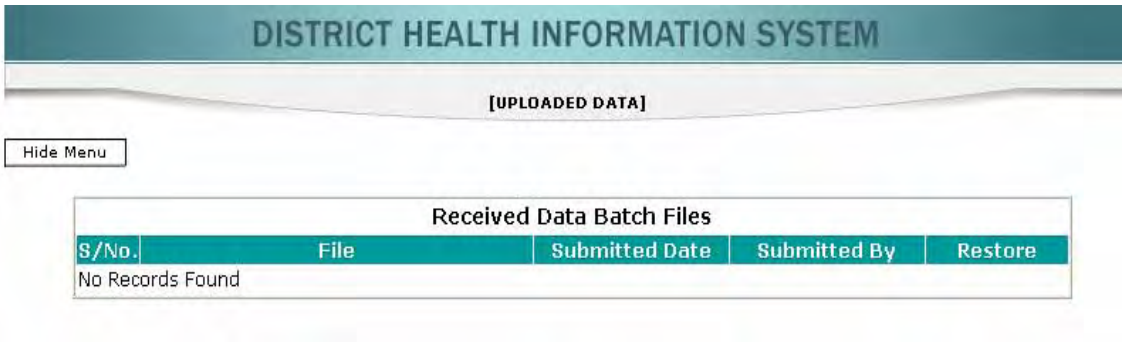
- Click new batch file to create new batch file for entered data.
- Click on Download link to download dump file of district entered data and save into disk.
- Now send this dump file to upper level for latest changes.

Note: This screen will use when Monthly report data enter for the month. After completion of date entry press new batch file to create batch file then dial to province server and upload this batch file to province server.

Downward Synchronization

Restore Received Data

When you will click on the ***Restore Received Data*** in Downward Synchronization menu, following screen will appear in front of you.

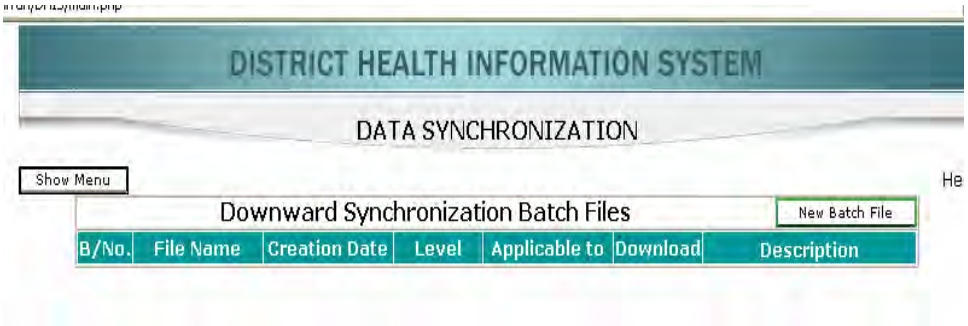


New received data will appear in list, restore data by pressing clicking on it

Note: when lower level upload data to upper level it will show in this screen just press restore button to merge in current database.

Create batch file (New forms).

When you will click on the ***Create batch file (New Form)*** in upward Synchronization menu, following screen will appear in front of you.



- Click new batch file to create new batch file.
- Click on Download link to download dump file of district entered data and save into disk.
- Now merge this file to current database by restore new forms.

Note: Click new batch file button to create new batch file for lower level. This file contains system setup and new data entry form for lower level.

Database Backup

When you will click on the ***Database Backup*** in the menu, following screen will appear in front of you.

1. Click backup button
2. It will save backup file in desktop
3. Copy that file and save it in safe place.

Note: it is recommended that save copy of file in other place too.

Restore Database.

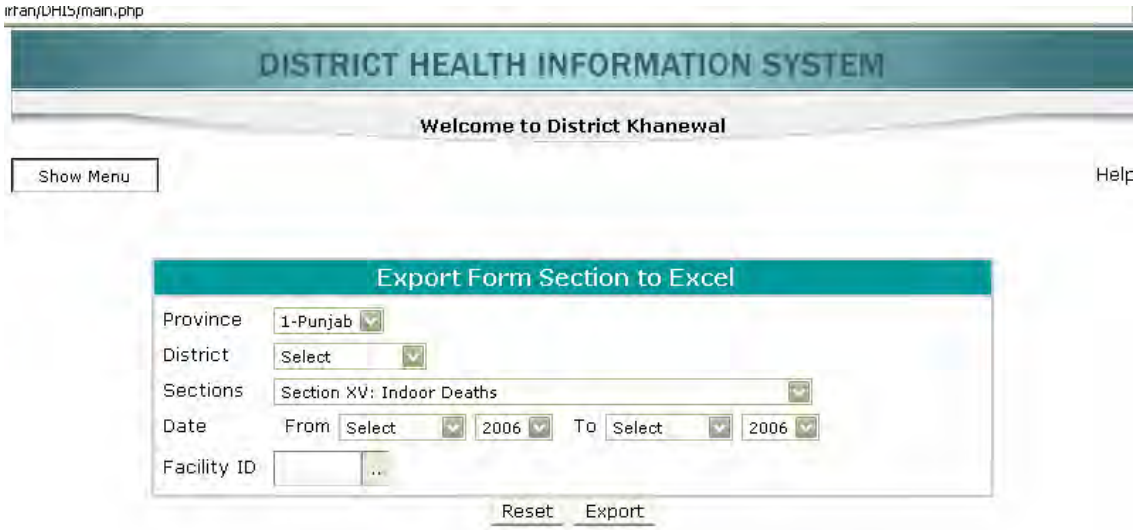
When you will click on the ***Restore Database*** in the menu, following screen will appear in front of you.

1. Click browse button to select already back up file.
2. Press restore button to restore old status in current database.
3. Press reset to clear file.

Note: Restore process will install the previous status of data before restoring make sure this operation does not loss your current data.

Export Data to MS Excel.

When you will click on the ***Export Data to MS Excel*** in the menu, following screen will appear in front of you.



1. Select province list
2. Select District from list
3. selection section
4. Date range in month/year
5. Facility ID.

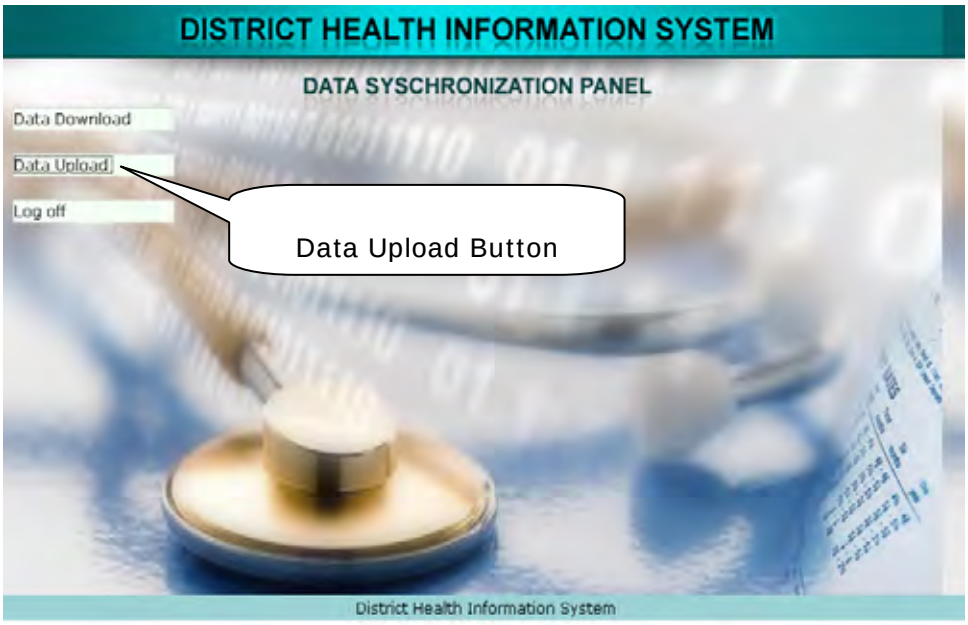
Note: it will export data to MS-excel format for further analysis on specified dates, section or facility.

Chapter – 11

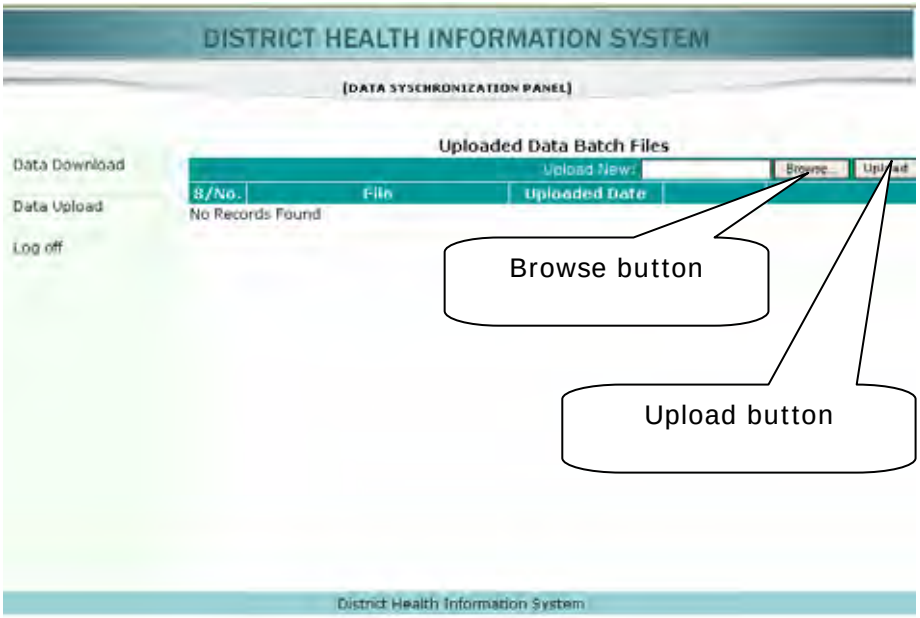
Data Uploading
&
Downloading

Steps to upload data to upper Level

1. Create (Save) Batch file of entered data.
2. Establish dialup connection to province level.
3. Open browser and province URL for application (e.g http://192.168.1.1/DHIS)
4. Provide Login name and password following screen in front of you.



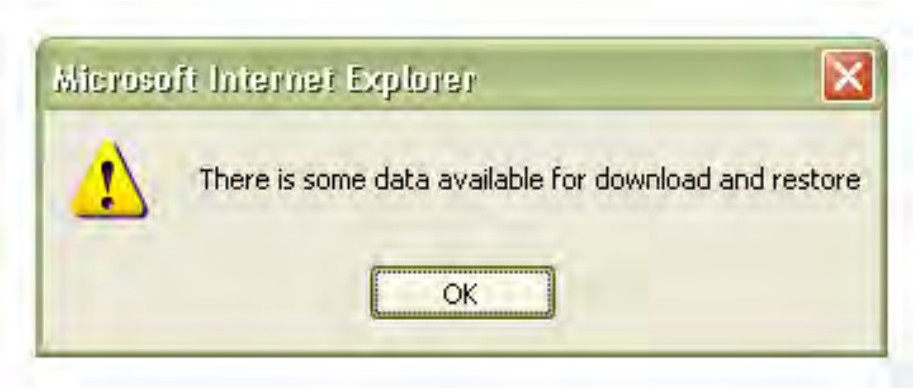
5. Click data upload button following screen comes infront of you



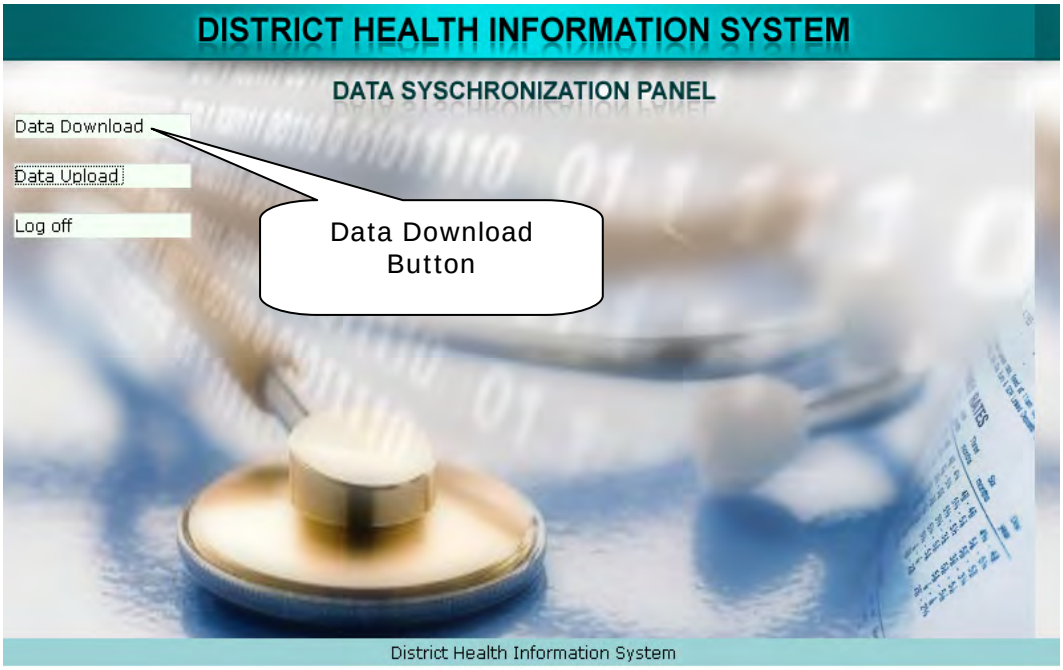
6. click browse button to select saved batch file
7. Press upload button to upload selected batch file to province level. Upload will take time, depend on dialup connection speed.
8. Once uploads complete file will list bellow
9. Now logoff and disconnect dialup connection.

Steps to download data from upper Level

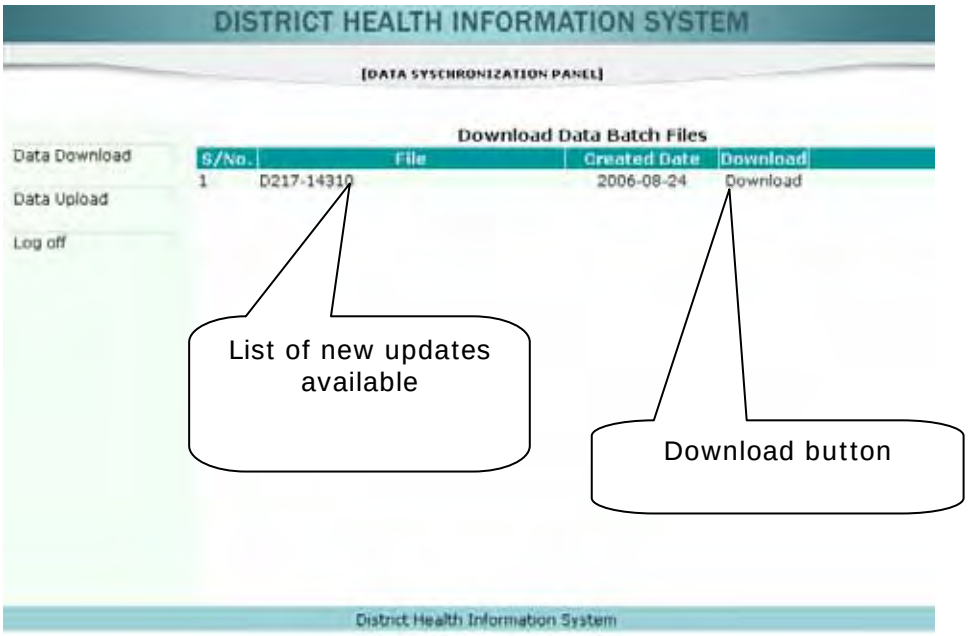
1. Establish dialup connection to province level.
2. Open browser and province URL for application (e.g http://192.168.1.1/DHIS)
3. Provide Login name and password following message in front of you.



4. press ok button following screen will appear



Click data download button following screen comes infront of you



5. Click download button and press save button dialog box will open to ask the location of data saving. Provide the location and press save button on dialog box, it will download selected file in specified path.
6. Press upload button to upload selected batch file to province level. Upload will take time, depend on dialup connection speed.
7. Once file has been downloaded now merge into your current database through ***restore forms (New forms)*** in sub-menu of upper level synchronization.
8. Now logoff and disconnect dialup connection.

Chapter – 12

Trouble Shooting

Trouble Shooting

Login to DHIS

Application does not login following problem can occurs

1. **Server is not Plug ON:** Make sure Server is properly switched ON.
2. **Network is not working:** Make sure the Network Cable is properly plugged into the NIC Card.
3. **Switch is not Plug ON:** Make sure the network switch is plugged ON.
4. **Server name or IP address is not correct:** Make sure the server name or IP address is correct (e.g http://192.168.1/DHIS or http://Servername/DHIS) and also make sure name of application is in capital letters (e.g DHIS)
5. **Client is not on network:** Make sure client network cable is properly plugged in to the NIC Card.

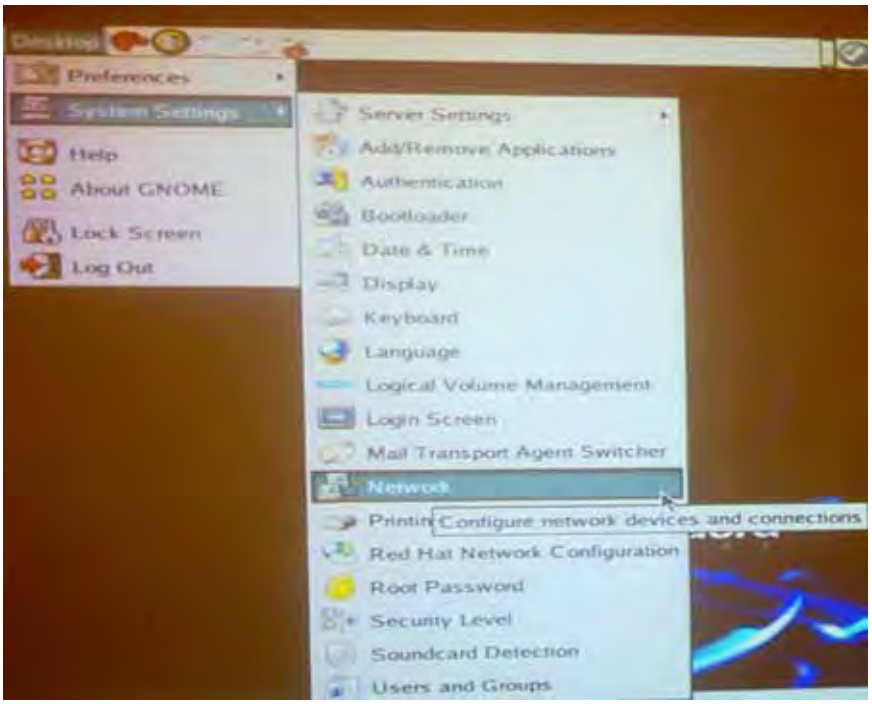
Network Configuration.

System is not on network following problems can occur.

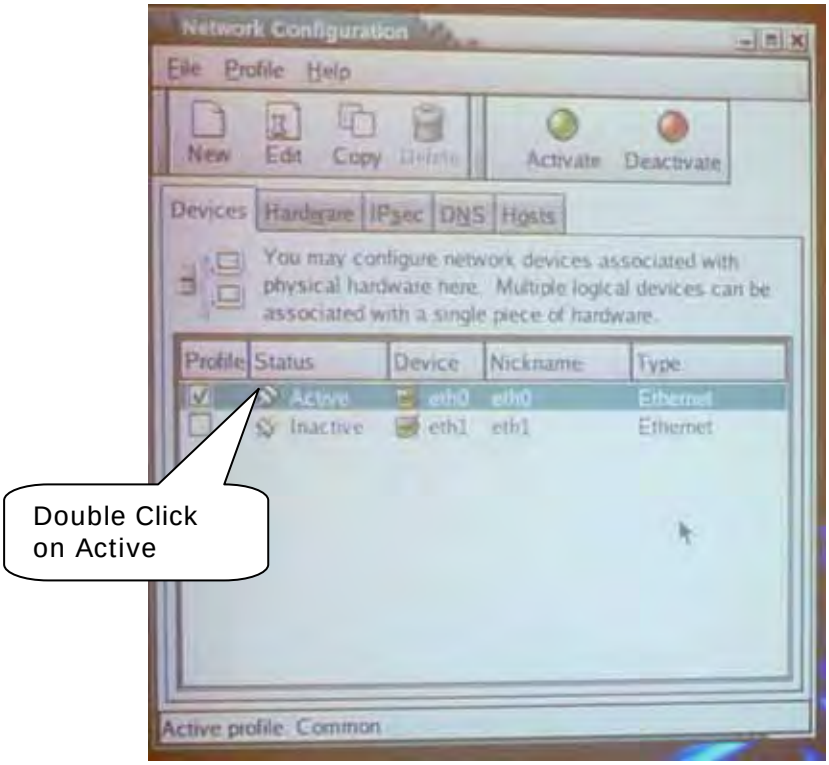
1. Network cable is not properly plugged into the NIC Card.
2. Network switch is not plugged ON.
3. Network configuration is not properly configured.

How to configure system in network.

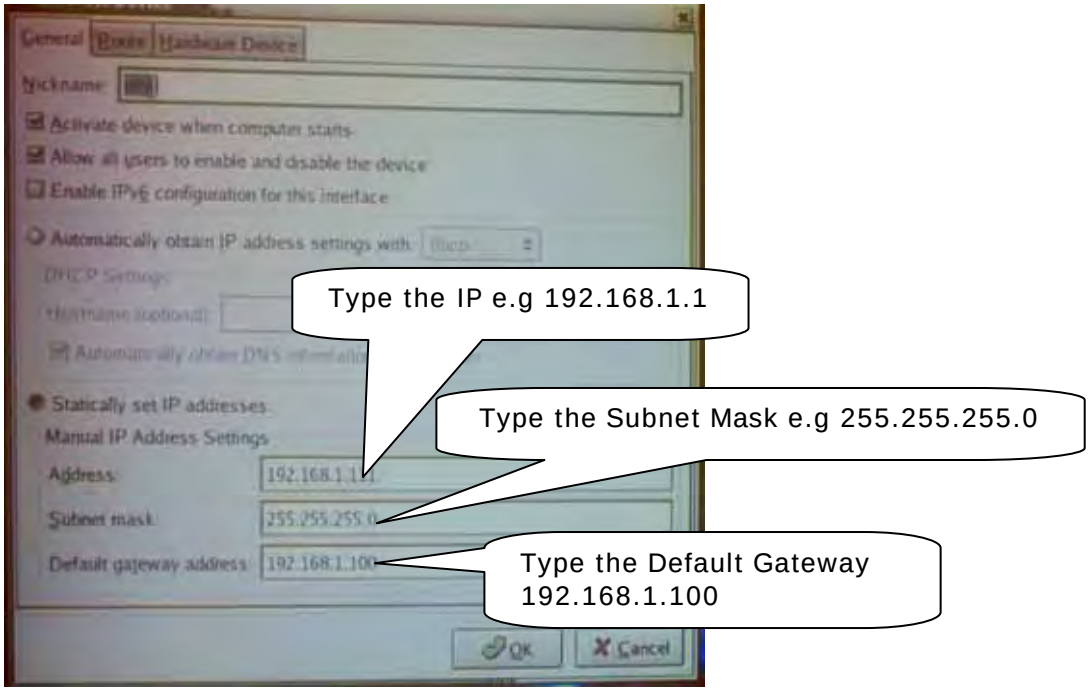
1. Turn on the network switch.
2. Turn on the Server.
3. Insert network cables in the NIC Card (Client Computer).
4. Click on Desktop menu in main screen.
5. Select option System Settings.
6. Click on Network.



Following Screen will appear in front of you.

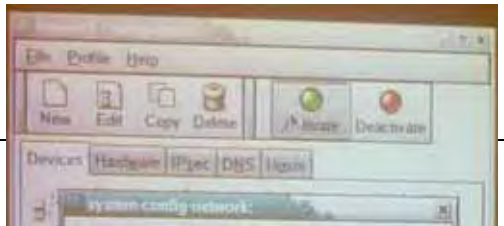


Double click the Active connection following screen will appear in front of you.



7. Set IP address, subnet mask, and default gateway address
8. Press ok to close this window

.



9. Click the Active Button the window appears click ok
10. Close network configuration screen.

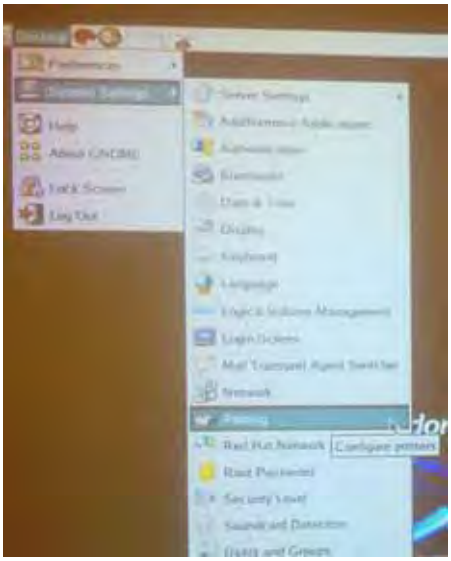
Printer Configuration

Printer is not working following problems can occur.

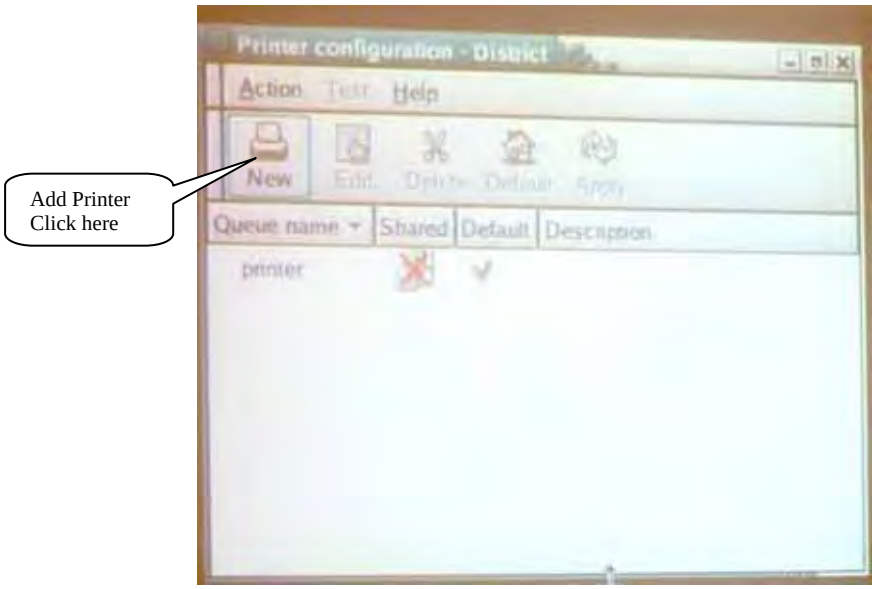
1. Printer is not plugged ON.
2. Computer is not plugged ON where printer attached.
3. Printer System is not on network.
4. Network switch is turned OFF.
5. Network Cable is not plugged properly into the NIC Card.

How to configure printer

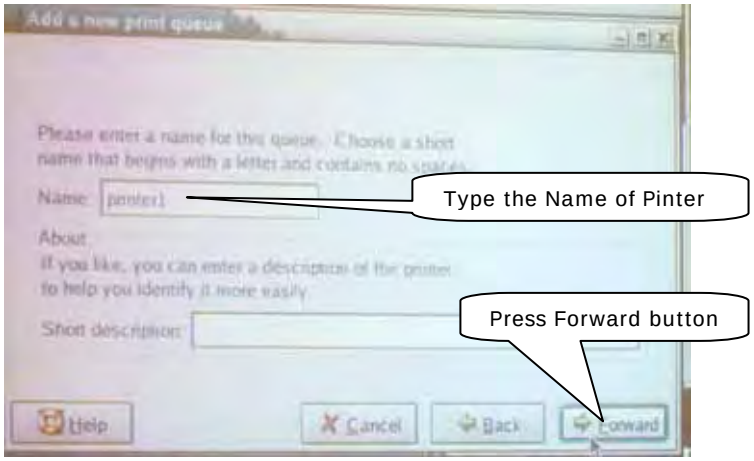
1. Turn on the computer where printer attached.
2. Turn on the printer
3. Properly turn on the network switch and make the network cable is plugged into the NIC.
4. Click on the Desktop menu in main screen.
5. Select the System Setting.
6. Click on the Printing option.



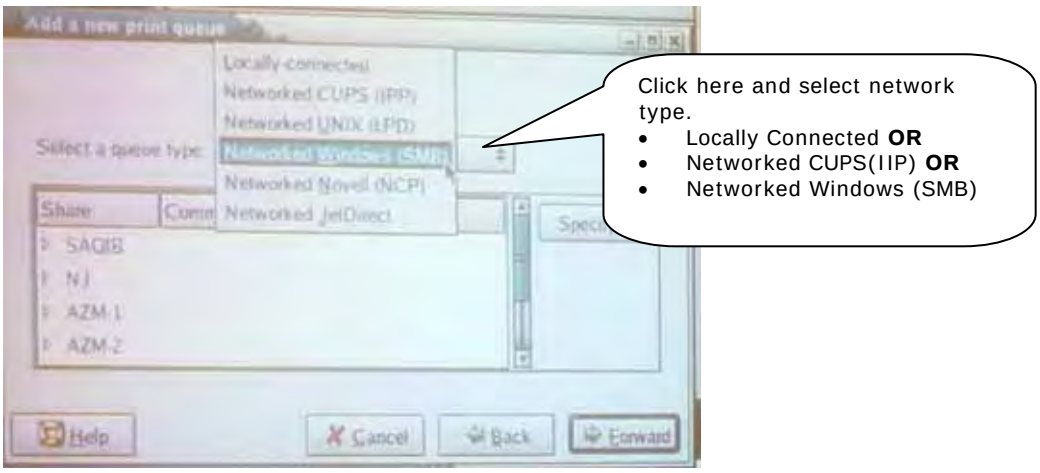
Following screen will appear in front of you



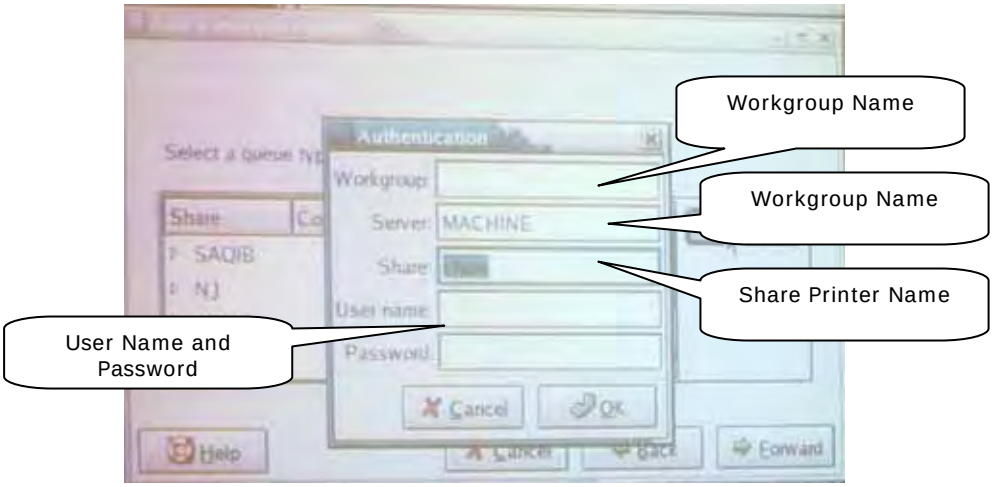
Click on the New button.



Add the printer for the network and forward

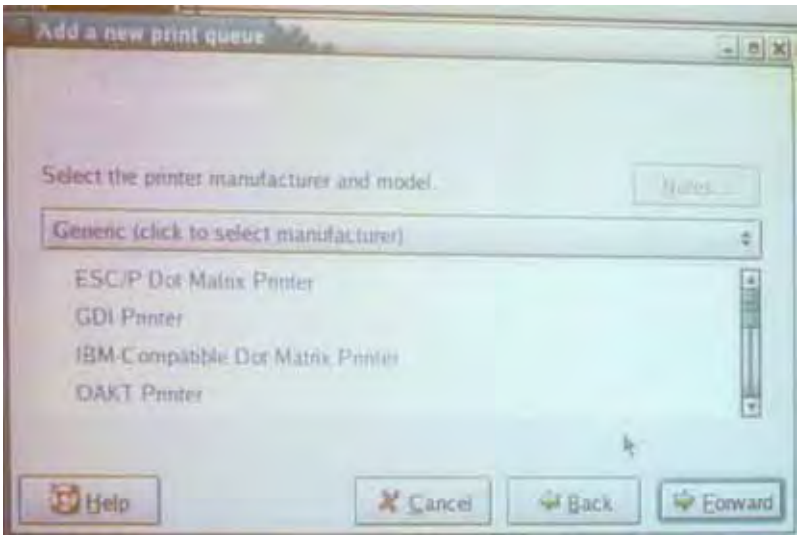


Click the **Network Window (SMB)** then enter Authentication.

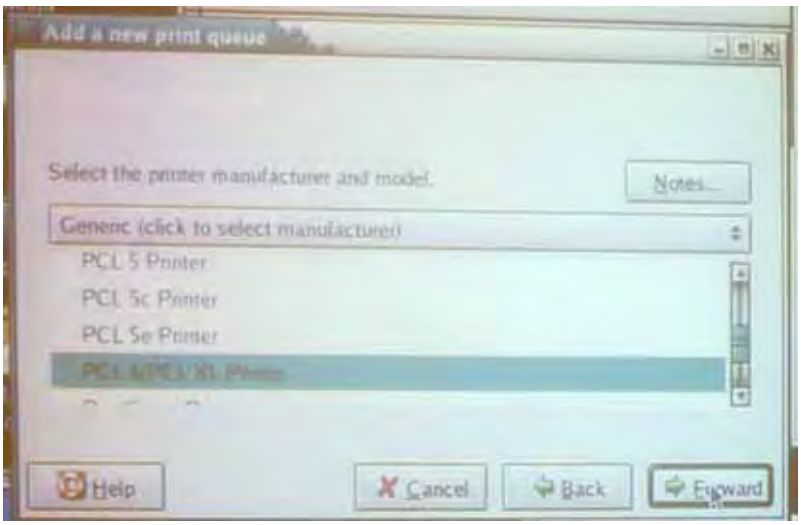


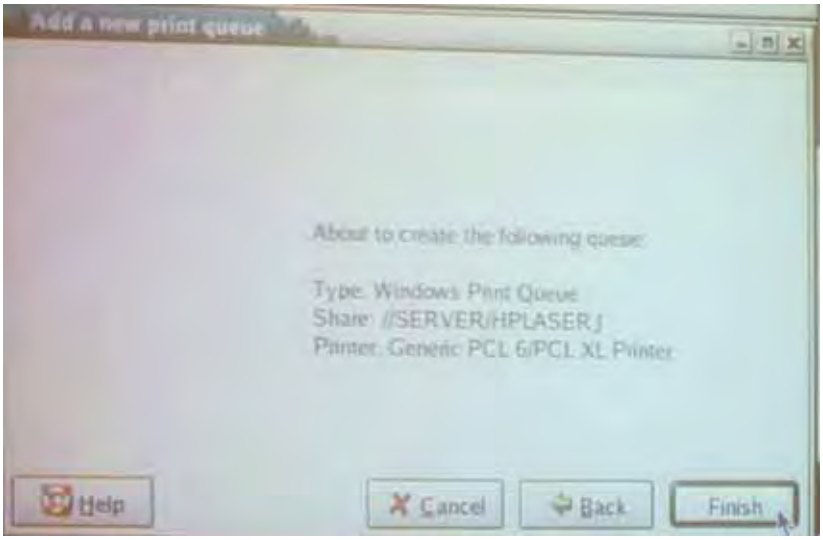
Type the name of workgroup, Name of Server, name of printer in share text box, user name and password to access the network printer and press ok to save authentication settings.

Add new printer if printer is not listed or press forward.



Select the PCI 6/PCL XL Printer and press forward.





Click The Finish Button to close printer configuration wizard.

END

PART III

INFORMATION SECURITY POLICY

District Health Information System

Sub Contracted Work on Computer System Development

for the Study on

Improvement of Management Information System in Health Sector in The Islamic Republic of Pakistan

Information Security Policy

Category	Information
Customer	System Science Consultants Inc.
Project	Development of District Health Information System
Document	Information Security Policy
Document Version	1.3
Document Status	Final
Identifier	SSC/DHISCheckList/9
Author(s)	AZM Technical Team
Approver(s)	SSC
Issue Date	October, 2006
Last Revision	4th December, 2006
Distribution	1. AZM 2. SSC

TABLE OF CONTENTS

1. INTRODUCTION - 4 -

2. INFORMATION SECURITY RISKS & THREATS - 6 -

2.1. SECURITY THREATS - 6 -
2.1.1. THREAT CONTROLS - 6 -
2.2. SECURITY RISKS - 7 -
2.2.1 QUANTITATIVE RISKS ASSESSMENT - 7 -
2.2.2 QUALITATIVE RISKS ASSESSMENT - 8 -
2.2.2.1 THREATS - 8 -
2.2.2.2 VULNERABILITIES - 8 -
2.2.1. RISK CONTROLS - 8 -

3. ROLES & RESPONSIBILITIES - 9 -

4. PROCEDURES & PROCESSES - 10 -

4.1. PHYSICAL SECURITY - 10 -
4.1.1. INVENTORY LIST - 10 -
4.1.2. HANDOVER & TAKEOVER OF INVENTORY - 10 -
4.1.3. ACCESS CONTROL - 11 -
4.1.4. POWER PROTECTION - 11 -
4.1.5. INSPECTION & PREVENTIVE MAINTENANCE - 11 -
4.1.6. PERIODIC INSPECTION - 12 -
4.1.7. PERIODIC MAINTENANCE - 12 -
4.1.8. PHYSICAL AUDIT - 13 -
4.2. DATA SECURITY - 13 -
4.2.1. ACCESS CONTROL & PASSWORDS - 13 -
4.2.2. PASSWORD COMPLEXITY REQUIREMENTS AND SAFE KEEPING - 14 -
4.2.3. ROLE BASED ACCESS PRIVILEGES - 15 -
4.2.4. DATA BACKUP - 15 -
4.2.5. VIRUS PROTECTION - 15 -
4.3. NETWORK SECURITY - 15 -
4.3.1. ACCESS CONTROL - 16 -
4.3.2. SERVER & CLIENT SECURITY - 16 -
4.3.3. FILE SYSTEM SECURITY - 17 -
4.3.4. INTERNET & DIALUP ACCESS - 17 -
4.4. INCIDENT REPORTING - 18 -
4.4.1. CHECKLIST FOR USER LEAVING UNDER GOOD CIRCUMSTANCES - 19 -
4.4.2. CHECKLIST FOR USER LEAVING UNDER OTHER CIRCUMSTANCES - 19 -
4.5. COPY RIGHTS - 20 -

5. USER LOG & MONITORING - 21 -

6. SECURITY AUDIT - 22 -

6.1. SECURITY AUDIT APPROACH - 22 -
6.2. COMMON AUDIT QUESTIONS - 23 -
6.3. MAJOR AREAS FOR SECURITY AUDIT - 24 -

ANNEXURE - 25 -

1.1. INVENTORY LIST - 25 -
1.2. STOCK TAKING SHEET - 26 -
1.3. HARDWARE MAINTENANCE LOG - 27 -
1.4. DHIS SOFTWARE UPDATE LOG - 28 -
1.5. VIRUS CHECKING LOG - 29 -
1.6. HARDWARE HAND /TAKE OVER FORM - 30 -
1.7. DATA BACKUP/RESTORE LOG - 31 -
1.8. USER & PRIVILEGES MANAGEMENT LOG - 32 -

1. INTRODUCTION

This document presents a proposal for a comprehensive Information Security Policy to be adapted by the managers of District Health Information System (DHIS) in the four provinces (Balochistan, NWFP, Punjab and Sindh) as well as the federal level. A consultative process would be necessary at each of the above locations/levels, involving senior officials from Health Departments, HMIS Coordinators/Managers, and data/network custodians/administrators to finalize specific policy documents and formulate standard operating procedures and define authority levels. Consultant can facilitate this consultative process and provide the necessary technical backup to frame province-specific policy guidelines.

District Health Information System (DHIS) processes and procedures have been derived from the best International Standards Practices; but non comprehensive; amendments and revisions as and when required and deemed necessary will be issued to meet the on-ground situation. All recipients of these procedures are advised that whenever any amendment/revision is issued, it must be incorporated in the information sheet so that it is kept up-to-date. Violation of these rules will be considered as misconduct and disciplinary action will be taken against the defaulters.

The District Health Information System (***DHIS)*** software application is built around the principle that all transactions are entered only once, whether at district level or its upper tire. It is a ***multi-location system***, with consolidation of data possible at the provincial/federal level for a reporting month. It is the central repository of health facilities performance, maintaining the highest summary level of HIS reporting information from the transaction details supplied by its lower level. All events that have a reporting or monetary impact is ultimately reflected in the DHIS.

The overall system comprises of different components, the DHIS software application will be implemented at different locations and will server the needs of following levels;

Implementation Level	Remarks
District	A District office will have option in the system to enter and generate reports based on all the data related to different facilities; in addition to that district will synchronize the data with upper level i.e. provincial server.
Province	A provincial office can have the access on the all the district data to review reports.
Federal	Federal can access the provinces data to review reports. Federal will also be responsible for the administration of the system policy and the procedures implementation and also for keeping standardization in the DHIS.

Strong and effective information security policy is integral part of any implementation where all the data is distributed and the qualified human resources is not available for the specialized task related to data/operation management. To address this need of information security and enable relevant level management for the application of security policy this document is developed, which is primary source of information about information security issues for the DHIS application software. It contains overviews as well as task and reference information. This document includes the following aspects:

Chapter 1 **Introduction:** describes the overview of Information Security Policy need.

Chapter 2 **Risks & Threats:** describes the associated information security risk & threats.

Chapter 3 **Roles & Responsibilities:** describes the mapping of operation roles & responsibilities.

Chapter 4 **Procedures & Processes:** describes the associated procedures and process for implementation of controlled operation environment.

Chapter 5 **Usage Log & Monitoring:** describes the tasks related to usage and also monitoring of proper use and audit trail.

Chapter 6 **Security Audit:** describes the activities for the security audit for effective implementation of information security.

This Information Security Policy is intended to help DHIS operation managers for implementing ongoing information security procedures and guideline document to establish standard operating procedures based on this policy that will be effective after the approval of competent authority and will be implemented accordingly.

2. INFORMATION SECURITY RISKS & THREATS

Protecting HMIS sections from outside threats is clearly important, but to protect the organization from internal threats is more important than extranet ones. All managers/administrators of respective levels will be provided a copy of the Information Security Policies and required to sign a statement that they have received them, read them, understand them, and agree to abide by them. This applies to all existing employees, contractors, temporary workers, etc., as well as all new personnel/data handlers.

2.1. Security Threats

An HMIS Computer Cell and the DHIS System is prone to different types of threats, out of which some may be "internal" and others can be classified as "external" threats. Internal threats may be caused due to the following reasons:

1. An employee or a consultant, someone who knows the weaknesses of the software being used or has the ability to introduce viruses into a system.
2. Employee or consultants someone who knows the advanced technological aspect of the software and can use outside system means to corrupt or modify the data/software.
3. Use of internet on the client of server comport.
4. Email attachments containing virus opened by novice users.
5. Employees with access to restricted areas; this may include the possession of unauthorized passwords. If something is password-protected, chances are there is confidential information involved
6. Laptops used by home-office workers, may have their security prevention turned off when remotely connecting.
7. Introduction of additional computer/network which is not safe and virus protected.

2.1.1. Threat Controls

System manager/administrator of HMIS cell will take following measure to reduce/stop the internal threats to the system;

1. Ensure internet is not connected through the server or client computers over the network.
2. Perform a security audit, or have one performed.
3. Unless the knowledge, experience and manpower exist in-house, consult an outside expert on audits, policies, and the subsequent security monitoring and prevention service.

4. Ensure adequate background checks on employees.

5. Establish a security policy, and enforce it. This includes implementing things like changing passwords often and restricting sensitive areas. This creates the right attitude toward information security in your office and clarifies the consequences of any found internal breach.

6. Use firewalls. Firewalls protect against unauthorized logins usually from the outside world, preventing hackers from logging on to your network.

7. Use virus scanning software. Attachments to e-mails received and passed around are the biggest reason for the spread of viruses.

8. Implement ongoing managed services.

9. Don't use or open file received from outside system, unless it is properly scanned for the viruses.

2.2. Security Risks

Security in any system should be commensurate with its risks. However, the process to determine which security controls are appropriate and cost effective is quite often a complex and sometimes a subjective matter. One of the prime functions of security risk identification is to put this process onto a more objective basis. Risks and threats related to information systems are of two types; ***Quantitative & Qualitative***, and it is essential for all information security manages in the respective HMIS offices to estimate their security risks and threats based on the above mentioned commonly used assessments procedures.

2.2.1 Quantitative Risks Assessment

This approach employs on two basic fundamental elements;

- The probability of an event occurring
- The likely loss it should occur

Quantitative risk analysis makes use of a single figure produced from these elements which can be calculated for an event by simply multiplying the potential loss by the probability. It is thus theoretically possible to rank events in order of risk and to make decisions based upon this. Only associated problem is unreliability and inaccuracy of the data. Probability can rarely be precise and can in some cases promote complacency. In addition controls and countermeasures often tackle a number of potential events and the events themselves are frequently interrelated.

2.2.2 Qualitative Risks Assessment

In this assessment for information security risks probability data is not required and only estimated potential loss is used, effective qualitative risk methodologies make use of a number of interrelated elements.

2.2.2.1 Threats

These are things that can go wrong or that can 'attack' the system. Examples might include fire or fraud. Threats are always there for every system.

2.2.2.2 Vulnerabilities

These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example fire vulnerability would be the presence of inflammable materials (e.g. paper).

2.2.1. Risk Controls

The steps include educating users to the threats, setting out policies that minimize the infection potential, installing block the internet use, regularly updated antivirus software, and installing all of the security patches for operating systems, web browsers, email clients, and applications. Having a single focal point for your information resources will streamline handling computer related issues; users will know who to ask for clarifications to policies and who to report violations to. These are the countermeasures for vulnerabilities. System managers/administrators can control risk by applying following methods:

- Deterrent controls reduce the likelihood of a deliberate attack.
- Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact.
- Corrective controls reduce the effect of an attack.
- Detective controls discover attacks and trigger preventative or corrective controls.

3. ROLES & RESPONSIBILITIES

Following roles and responsibilities are mapped specially keeping in view current provisions available in DHIS software:

Role	Level	Role can be assigned to	Responsibilities
Administrator	Federal	Technical officer (Software)	User management Form Management Data Management Installations & Trouble Shooting
	Province	Computer Program Officer / In charge HIS wing	User management Form Management Data Management Installations & Trouble Shooting
	District	District Coordinator DHIS	User management Form Management Data Management Installations & Trouble Shooting
Executive	Federal	DG Health Executive Director NHIRC	Monitoring of priority indicators Performance Evaluation Target Setting
	Province	Secretary Health Director General Health Services	Monitoring of priority indicators Performance Evaluation Target Setting
	District	Executive District Officer (Health) District Officer (Health) Medical Superintendent	Monitoring of priority indicators Performance Evaluation Target Setting
Operator	Federal	Data Entry Operator / Computer Operator	Report Generation Feedback Reports
	Province	Data Entry Operator / Computer Operator	Report Generation Feedback Reports Data Synchronization
	District	Data Entry Operator / Computer Operator	Data Entry Report Generation Feedback Reports Data Synchronization
Guest	Federal	Data Entry Operator / Computer Operator	Not Applicable
	Province	Data Entry Operator / Computer Operator	Data Synchronization
	District	Data Entry Operator / Computer Operator	Data Synchronization

4. PROCEDURES & PROCESSES

4.1. Physical Security

In order to maintain the physical security of computers i.e. to safeguard against thefts, tempering and insuring proper working, a well defined procedure is required for the following:

4.1.1. Inventory List

Inventory list must be prepared at all HMIS Cells for the record keeping of the existing computer hardware resources, and future purchases. Inventory can be maintained for both consumable like printer toner, printing paper etc and fixed assets like CPU, monitor, printer etc. System administrator of HMIS cell should be made responsible for maintaining the inventory list and also on pre-defined and surprise stock taking must be conducted by senior management of respective office.

Most common consumable Computer Accessories such as toners, floppy diskettes, CD's etc. must be kept in stock. End users will get the required item as and when required upon proper "Request Form". However all computer users are supposed to utilize computers in careful way so that life of each component of computer will be high and they are accountable for any miss use of Computers, printers and accessories. A sample inventory list is attached with this document as Annexure.

4.1.2. Handover & Takeover of Inventory

Any existing or newly appointed HMIS cell employee(s) upon joining will be provided with the required hardware after approval from their respective head of the department. Similarly, any leaving employee will have to return all the issued items. The proposed handing & taking over process is defined here;

1. The user puts up the "Requisition Form" for the required hardware duly approved by the respective Head of the Wings. Signature of employee & Head of the Wings on Requisition Form is must.
2. If the desired requisition is approved by head of the Wing, the same is forwarded to the responsible for the necessary action. Authorized person assesses the User requirement and decides on the Hardware & Software.
3. The Network Technician of the MIS section will configure the hardware and installs the necessary software on the machine.
4. The Assistant Network Administrator will arrange the printing facility either through LAN printer or locally.

5. Once the user has received the machine, the Network Technician will record the following info on "Installation/Inspection/Maintenance Sheet". Support Staff & User will sign the sheet (See Annexure).
6. Every machine will have a separate "Installation/Inspection/Maintenance Sheet".
7. In case the Head of the Wing does not approve the hardware requisition then the same is intimated to the user and the MIS section considers the case closed.
8. In case the user request for specific software that is not available with MIS section then User need to initiate a request on "Request Form" and after approval by the Head of the Wing it will be purchased through the necessary procedure.
9. All Computers, monitors and printers etc. installed in HMIS Cell will be given discrete Serial Number. Each major item such as CPU, Monitor and printer/ plotter must have a Tag which must contains the serial number. And same is recorded in the "Installation/Inspection/Maintenance Sheet" (See Annexure).
10. As a result of transfer, retirement, resignation or removal from service of an employee, the HMIS Cell will ensure that all the returnable items issued to an outgoing employee are received back.

4.1.3. Access Control

Server computer & networking equipment i.e. switch or hub should be placed at secure place to avoid any intentional or unintentional attempt to destroy the computer hardware, and also from other natural disasters like rain, fire, earthquake etc. Only authorized person should be allowed for the maintenance activities of the server. All respective users of the client computer/workstations should be made responsible for the physical access to their hardware equipment and made responsible for physical security.

4.1.4. Power Protection

Proper electrification is essential in the offices where server and client computer will be placed. To protect server hardware, its operating system & DHIS application including database from any harm due to power failure or bad power supply, UPS should be installed with the server computer and (where ever possible with the client also). To protect client computers from electric surge, each client can be connected through good quality stabilizer. System administrator must ensure the power supply condition and wiring, lose connection/sparking can be harmful for computer hardware and attached accessories.

4.1.5. Inspection & Preventive Maintenance

To record the status of hardware issued and in-hand, periodic inspection will be carried out on quarterly basis (or required frequency). Hardware Preventive Maintenance will be carried out on monthly basis and any emergency breakdowns will be dealt based on contingency plan.

4.1.6. Periodic Inspection

Following point should be considered as important for inspection;

- The manager/administrator of HMIS Cell will perform the physical periodic inspection and will update the hardware "Inventory Stock Taking Sheet" from the "Inventory Sheet".
- The HMIS Cell reconciles the output of Stock Taking Sheet with the actual and record.
- The HMIS section will maintain a log book. All record has to be maintained so that it can be produced for audit purpose as and when required.
- All exceptions should be reported to senior management after completion of inspection as a summarized report.

4.1.7. Periodic Maintenance

Maintenance of hardware or software must be done as a result of inspection if required. Maintenance should also be a controlled process. The preventative maintenance will be carried out on monthly basis by administrator of HMIS Cell as follows:

- The preventative maintenance will be carried out on monthly basis by administrator of HMIS Cell.
- Concerned person involved in the periodic maintenance will fill the "Hardware Log Sheet" with its observations.
- In emergency breakdowns of hardware/software, the complainant (User) informs the HMIS Cell of the problem through placing a call at telephone or sending E-mail related to defect.
- System manager/administrator will register the complaint on the "Complaint Sheet" and will attend the complaint.
- After resolving the problem the System manager/administrator gets a sign off from the user.
- In case the problem could not be solved internally then outside firms are engaged following the necessary approval procedures.
- Once the firm is selected the HMIS cell hands over the equipment to the firm and records the movement on the "Hardware Log Sheet".
- Upon the return of the equipment, the system manager/administrator of the HMIS cell will receive the equipment and will check and then sign off.
- The system manager/administrator will install the equipment on its original place.

4.1.8. Physical Audit

The physical audit of equipment is one of the major components of the physical security and also provides periodic stock taking of the resources to maintain the inventory of the equipment, which again includes consumables and fixed assets. For this purpose of stock taking, stock taking sheets can be prepared based on last inventory list and quantity and condition can be filled during the physical audit.

4.2. Data Security

The most important area in the data security is the access control to particular information and also prevention of data from any physical/logical problem.

4.2.1. Access Control & Passwords

Authorised user of the DHIS will only access the computer system and then the DHIS software application and system administrator will maintain the privileges and prepare logins as per requirements; below mentioned steps will be followed to secure the access to the application and data;

- Users must logon to the HMIS Cell network domain with their authorized User ID and Password provided by the Network Administrator. No other domain or local login will be allowed.
- Users must change their passwords periodically or when the system prompts for a password change after certain interval of time set by Network Administrator. The maximum age of password is 90 days and after 87 days, the system would automatically remind/prompt users to change their password.
- Users are not allowed to share or disclose their password with anyone as this may lead to severe password misuse.
- The Minimum password length is 6 characters.
- Users cannot repeat last 6 passwords.
- User Account will be locked out on 5 bad logon attempts and will only be unlocked by Windows System Admin Team.
- If an account or password is suspected to have been compromised, then the password change procedure (policy) should be considered to change that password.

4.2.2. Password complexity requirements and safe keeping

Passwords must be selected in such a way that easy guessing of password is not possible. User administrator must inform the user about the following complexity requirement of password as well as for the password safe keeping.

Poor, weak passwords

Poor passwords can lead to easy guessing of the passwords and can be of following types:

- The password contains less than six characters.
- The password is a word found in a dictionary (English or foreign).
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, software, etc.

Strong passwords

It is recommended that strong passwords should be used to avoid heuristics and easy guessing techniques of hacking passwords. Strong passwords are of following types:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least six alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

Password Protection Standards

All passwords are to be treated as sensitive, confidential information.

Here is a list of "don’ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message

- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the HMIS cell.

4.2.3. Role Based Access Privileges

System administrator will assign the privileges based on the activity he/she has to perform in the system. Only new user will be assigned the rights from the approval of competent authority assigned for this. Following roles are envisaged for users;

- Administrator
- Operator
- Executive
- Guest

Any user who will be created using DHIS software application will be assigned any of above role and on his login system will start providing options/functionalities assigned to that role in the system.

4.2.4. Data backup

System administrator will be responsible for the periodic data backup and disaster recovery of the system in case of any disorder. He will maintain the data backup log in the format provided in the Annexure and relevant level head will do surprise check of that log and will note his remarks during the checking.

4.2.5. Virus Protection

System administrator will be responsible for all the required measures need to be done for the virus protection, which includes installation of the anti virus software and its update version on the server and client computers. All virus-infected file will be marked as “Quarantine” for one week after which the file will be automatically deleted.

4.3. Network Security

Following aspects should be considered by System manager/administrator for the network security;

4.3.1. Access Control

Administrator of the system will take following measure for secure access over the internal network;

- All Heads of Departments or Supervisors must ensure that Users under their supervision who are authorized to use the Desktop are fully aware of and comply with the information security policy.
- All Desktop users must ensure that they fully understand and comply with the information security policy in their individual capacities and will keep themselves aware of any updates/changes.
- Users are not allowed to move/relocate Desktops from their designated place and department and if such movement is necessary, Head of the section will be informed prior to the movement for help and guidance.
- Users are not allowed to connect/plug-in/install any extra piece of hardware to any available port (comm., USB, ISA or PCI) either internal or external within the Desktop without prior permission of Network Administrator.
- Users are not allowed to eat, drink or smoke near the Desktop as it may cause damage to the Desktop.
- Users are not allowed to play computer games and engage in any other kind of entertaining activities on their Desktops.
- Users should connect their Desktops only with UPS available power points.
- Any problem related with the Desktop should be reported to System manager/administrator through telephone or email/defect report.
- All access to the Desktop hardware setting including the sensitive BIOS setup will be administer by System Administrator and that users are not allowed to access or change these settings as this may cause improper functioning or complete halt/crash of the Desktop. CMOS/BIOS setting password will be kept by System Administrator.

4.3.2. Server & Client Security

Depending on the user role, administrator of the system will take following measure for server and client security;

- Depending on the physical location, all desktops must be joined with their respective domains.
- Users will be allowed to logon to their assigned Desktop only
- Users are accountable for what is being done on their Desktop with his/her User ID. User must lock their Desktops before leaving their workplace for any length of time.
- If multiple users are sharing a single Desktop, then each user will login by his/her unique User ID and password and must logout before leaving the Desktop.
- Users are not allowed to keep or inquire upon the local administrative passwords of the Desktops. Only Network Administrator will hold such passwords and under ***special operational requirements,*** such

passwords or equivalent administrative rights will be given only after approval from the appropriate authority of the user.

- In such cases the following applies:
    - User will be required to provide written approval from their respective authorities, those special operational needs, which require such privileges.
    - User will not misuse the password in any circumstances by installing or removing software or by altering other Desktop configurations
- Network Administrator has the full right to revoke such privileges in case of non-compliance.

4.3.3. File System Security

Following file system security must be implemented and assured by the network administrator:

- In order to have a Data & Information security on LAN only approved Data & Information by the section head will be shared.
- NTFS level security will be implemented. Users will only have change rights on "user partitions/User folder" (partitions other then system partitions).
- Users are not allowed to share their local hard drive(s)/folder(s) for information sharing among the colleagues. For such sharing of information, central file server may be used with the help of Network Administrator.
- Users are responsible for taking back ups of their critical data residing on their local hard drive.
- Network Administrator has the right to share or un-share any folder without the prior permission of the User.
- Each user will have a default server-based personal roaming space of size 100 MB, where they can store critical data. Requests for additional server space beyond the default limit must be requested through the MIS section.
- Once a user's space reaches 90 MB in size, the user will receive a warning message. The user must delete unneeded files from Central file server after taking backups of critical data.

4.3.4. Internet & Dialup Access

Internet access through the DHIS server or client will not be allowed to any type of users. Following will be ensured;

- Users will not allow plugging their personal home computers on HMIS CELL network under any circumstances.

- Users are not allowed to use their Desktops as a tool for accessing other systems on the network without any purpose within and outside HMIS CELL and for which they are not entitled to be as authorized users.
- Users are not allowed to connect their Desktops with the Internet using any dialup modem connections.

4.4. Incident Reporting

This section is meant to provide some guidance for internal situations. The most common mistake made by organizations is to attempt to process a computer themselves. While Information Resources personnel may be able to recover deleted files in almost all instances they will not have the training and tools necessary to properly examine a computer.

The mere process of allowing a subject computer to boot can irrevocably destroy evidence. Therefore, it is important to know which files the individual accessed in their last days. Failure to follow the guidelines results in these dates being overwritten. The best time to have a computer examination conducted is when the employee first comes under suspicion. The examination can often be done secretly, thereby not alerting the employee. Assuming that the organization already has the appropriate policies in place, key-logging or screen capture software can be secretly placed on the suspect's computer. Key-logging software captures all of the keystrokes that are made. Screen capture software takes a "snapshot" of what is on the computer monitor at a preset interval. The information from either type of program can be stored on the local hard drive, stored on a network drive, or transferred virtually anywhere via the Internet. Software is also readily available that allows the suspect's computer screen to be monitored remotely in real time.

If the employee has just resigned, the best policy is to have a trusted employee secure the computer(s) used by that individual. Do not allow anyone to access the computer(s) in any manner. A qualified computer examiner should be sought out and the hard drive(s) turned over to them for processing. Likewise for any removable media that might contain evidence. Any server log files that could possibly contain information about the employee's actions should be immediately copied and preserved. Any files that might be stored on a network drive and any email that might be stored on a server should be immediately copied and preserved. Any backup tapes that could contain evidence should also be preserved. In the event that an employee is to be fired, these procedures should be undertaken while the employee is in the office being fired. The employee should not be afforded any further access to computers or storage media (i.e.: diskettes, CD-ROMs, etc.).

While it is likely that an employee who submits their resignation has already made copies of whatever data and information they plan to take with them, giving them further access to anything sensitive is very dangerous. Immediately upon submitting their notice, the employee should lose all email, Internet, and network access. If

their workstation contains anything sensitive, they should lose access to that also. Disgruntled employees have been known to send out company-wide emails and/or delete massive amounts of data on their last day. Anytime an employee leaves the organization, for any reason, all computer accounts that the individual had access to should be immediately closed or have new passwords installed.

4.4.1. Checklist for User Leaving under Good Circumstances

Good circumstances can be defined as an employee leaving with the consent of management and with prior notice. Following must be assured before user leaves the organization:

- Close all email and user accounts that were unique to the user.
- Change all passwords on shared systems that the user knew.
- Ensure that all copies of sensitive information are retrieved from the user.
- Change the password on any voicemail systems the user had access to and change the message appropriately.

4.4.2. Checklist for User Leaving under Other Circumstances

Employees leaving suddenly or without prior information may carry the sensitive information of organization with them. Therefore it is important that following steps must be taken to ensure the confidentiality of information:

- Close all email and user accounts that were unique to the user
- Change all passwords on shared systems that the user knew
- Ensure that all copies of sensitive information are retrieved from the user
- Change the password on any voicemail systems the user had access to and change the message appropriately
- Upon notification (firing or resignation), do not allow the user any further access to any computers, disks, files, etc.
- Secure all computers that the user was assigned (workstation, laptop, etc.). All of the user's removable media should likewise be secured. They should be locked up in a manner such that an absolute minimum of people have access to them, preferably just the individual seizing them.
- Secure all server logs that might contain evidence. This includes: file accesses; application accesses; print jobs; email; and Internet access. This should be done by burning them onto CD.
- Secure all of the user's files on any network drives. This should be done by burning them onto CD.
- Secure any email that might be stored on the network.

- All backup tapes that could possibly contain any evidence should be secured with the computer(s) and removable media.
- Obtain and secure all of the user's available telephone records (long distance, cellular, etc.

4.5. Copy Rights

The HMIS Cell shall respect the intellectual property rights and prohibit the following on its premises, computers and storage media the following pirated (illegal copies) materials:

- Operating System
- Third Party Software Applications
- Entertainment materials including: music, movies, games, etc.
- Reading materials including books, journals, etc. (hard or soft-copy)

These materials shall not be:

a) Brought in from outside

b) Copied from other medial

c) Stored on media

d) Downloaded from internet in the HMIS premises or computers.

This is with the exception of software and print materials available in the public domain such as the software and books available/copied/downloaded under GNU Public License, such as Fedora, Mozilla Firefox, etc.

5. USER LOG & MONITORING

System provides means to do the logging of usage of software. Different user's login and log out time as well as the transactions in the software made can be viewed with time and date stamps. It is responsibility of system administrator to ensure and monitors the proper usage of software that includes

- Making sure that no user logged in after office times
- Users logged in only to those machines that were assigned to them
- Users kept the backup of their data
- Users did not attempt to install un allowed software's or hardware's

6. SECURITY AUDIT

A computer security audit is a systematic, measurable technical assessment of how the organization's security policy is employed at a specific site. Computer security auditors work with the full knowledge of the organization, at times with considerable inside information, in order to understand the resources to be audited. Security audits do not take place in a vacuum; they are part of the on-going process of defining and maintaining effective security policies. It involves everyone who uses any computer resources throughout the organization. Given the dynamic nature of computer configurations and information storage, security audits provide such a tool, a fair and measurable way to examine how secure a organization and its information really is.

6.1. Security Audit Approach

Before the computer security auditors even begin an organizational audit, there's a fair amount of homework that should be done. Auditors need to know what they're auditing. In addition to reviewing the results of any previous audits that may have been conducted, there may be several tools they will use or refer to before.

- The first is a site survey. This is a technical description of the system's hosts. It also includes management and user demographics. This information may be out of date, but it can still provide a general framework.
- Security questionnaires may be used as to follow up the site survey. These questionnaires are by nature subjective measurements but they are useful because they provide a framework of agreed-upon security practices. The respondents are usually asked to rate the controls used to govern access to IT assets. These controls include:
  - ✓ Management controls
  - ✓ Authentication/access controls
  - ✓ Physical security
  - ✓ Outsider access to systems
  - ✓ System administration controls
  - ✓ Procedures
  - ✓ Connections to external networks
  - ✓ Remote access
  - ✓ Incident response
  - ✓ Contingency planning

Site surveys and security questionnaires should be clearly written with quantifiable responses of specific requirements. Auditors, especially internal auditors, should review previous security incidents at the organization to gain an idea of historical weak points in the organization's security profile.

The auditors will develop audit plan. This plan will cover how will audit be executed, with which personnel, and using what tools. They will then discuss the plan with the authorities. Next they discuss the objective of the audit with site personnel along with some of the logistical details, such as the time of the audit, which site staff may be involved and how the audit will affect daily operations. Next, the auditors should ensure audit objectives are understood.

6.2. Common Audit Questions

Computer security auditors perform their work though a personal interview, vulnerability scans examination of operating system settings, analyses of network shares, and historical data. They are concerned primarily with how security policies - the foundation of any effective organizational security strategy - are actually used. There are a number of key questions that security audits should attempt to answer:

- Are passwords difficult to crack?
- Are there Access Control Lists (ACLs) in place on network devices to control who has access to shared data?
- Are there audit logs to record who accesses data?
- Are the audit logs reviewed?
- Are the security settings for operating systems in accordance with accepted industry security practices?
- Have all unnecessary applications and computer services been eliminated for each system?
- Are these operating systems and commercial applications patched to current levels?
- How is backup media stored? Who has access to it? Is it up-to-date?
- Is there a disaster recovery plan? Have the participants and stakeholders ever rehearsed the disaster recovery plan?
- Are there adequate cryptographic tools in place to govern data encryption, and have these tools been properly configured?
- Have custom-built applications been written with security in mind?

- How have these custom applications been tested for security flaws?
- How are configuration and code changes documented at every level? How are these records reviewed and who conducts the review?

These are just a few of the kind of questions that can and should be assessed in a security audit. In answering these questions honestly and rigorously, an organization can realistically assess how secure its vital information is.

6.3. Major Areas for Security Audit

Security audit will include following:

Antivirus audits: Network administrator is responsible to assure that latest version of anti-virus is working on all machines. This includes

a. Checking for latest downloads
b. Making sure it is up and running on all PC's
c. Keeping the log of when all the PC's were checked with date and name of machines

Backup audits: Data that needs periodic (daily, weekly or monthly) backup has been stored on the back up drive. This should be checked on periodic basis and log must be maintained when the last audit was done.

Hardware audit: Network administrator must conduct periodic and surprise audits at different machines to ensure that no one has installed a hardware that is not allowed such as on USB Ports or CD ROMS. It should also include checking that no hardware is missing from the facility.

User access audit: Network administrator must ensure on periodic basis that software and data has been accessed only by the users to whom that are relevant and data is not accessed on after office times.

ANNEXURE

1.1. Inventory List

Sr. No.	Item Description	Specification	Date of Purchase	Remarks

1.2. Stock Taking Sheet

Date of Stock Taking _____

Sr. No.	Item Description	Specification/ Condition	Quantity as on Record	Actual Quantity	Remarks

1.3. Hardware Maintenance Log

Hardware Item _____

Sr. No.	Reporting Date	Maintenance Type	Action Taken	Problem Solving Date	Remarks

1.4. DHIS Software Update Log

Sr. No.	Date of Update	Version/Build Number	Updated Features	Updated By	Remarks

1.5. Virus Checking Log

Sr. No.	Date	Computer Name	Virus Software	Remarks

1.6. Hardware Hand /Take over Form

Date	
Location	
Authorised By	
Handover Over By	
Take Over By	

Sr. No.	Item Description	Specification	Quantity	Condition

Signature_____ **Signature_____**

1.7. Data Backup/Restore Log

Sr. No.	Date	Backup/ Restore	Physical File Name	Purpose/ Remarks	Authorised By

1.8. User & Privileges Management Log

Sr. No.	User	User Type	Module	Authorised By	Rights Assigning Date

JICA