

System Overview: ePPOC Data Collection

Version 1.2

Contents

Overview of the System	2
Minimum Requirements and Installation Scenarios.....	3
Minimum Hardware and Software Requirements for Client Machines	3
Supported Installation Scenarios	3
REDCap.....	3
System Installation and Configuration.....	4
Installation	4
Configuration	4
Further Details about Configuration.....	5
Creation of the SQL Server Database.....	5
Creating the database using the application's 'Database Configuration Wizard'	5
Creating the database in SQL Server directly using the Create Database script	5
Configuration of the SQL Server Database	5
Configuration of the Desktop Application's Database Connection	5
Security Model	6
SQL Server Security	6
Application Layer Security.....	6
Application Update Model.....	6
Data Storage Requirements	6

Overview of the System

AHSRI will implement 2 systems for managing ePPOC data:

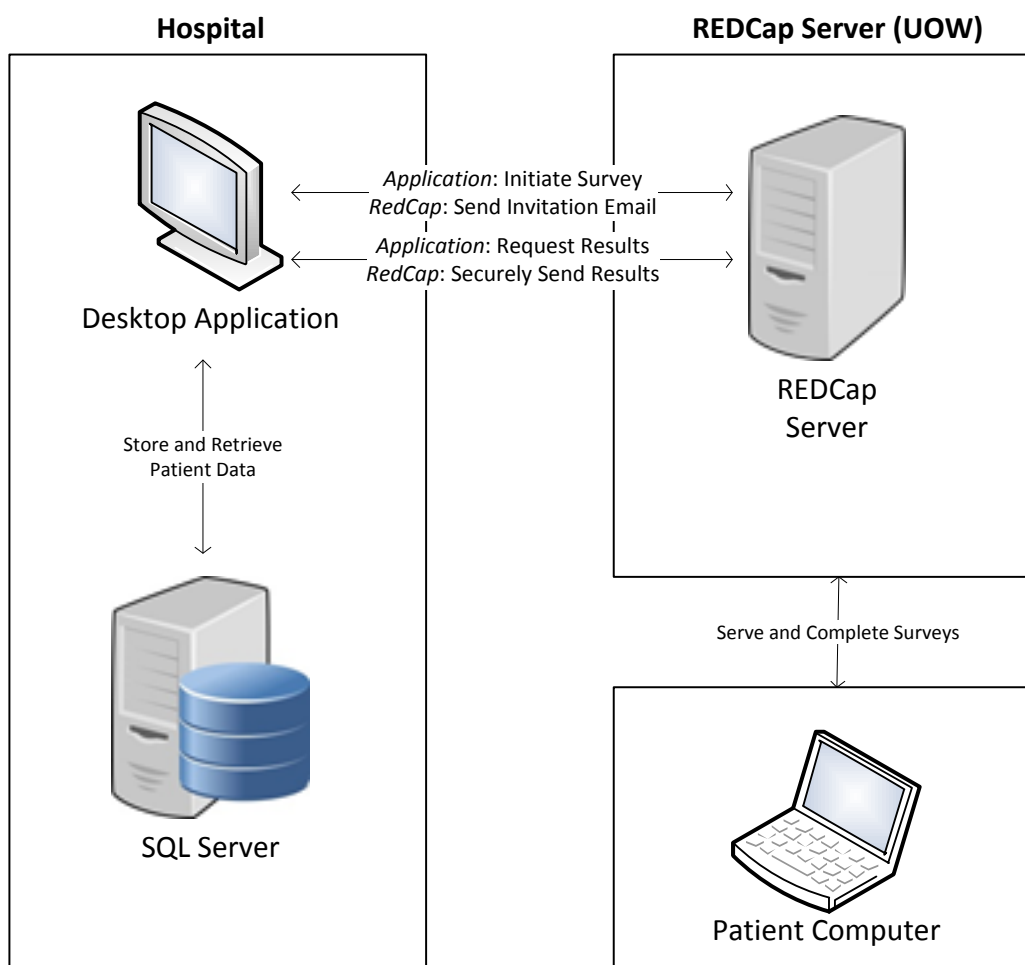
- **Data Collection System:** This is the system we will describe in this document. It consists of a desktop application (called epiCentre) and a web application (called RedCap). These systems are integrated and will be used for data entry and reporting of Patient, Episode, Pathway, Service and Survey information.
- **Data Collation System:** This system will allow AHSRI to collate, store and manage the de-identified data. It will be hosted and operated by AHSRI and will not require any installation at the hospitals.

The purpose of this document is to outline the requirements and design of the Data Collection System.

The Data Collection system can be divided in 2 components:

- **epiCentre - desktop application:** This application will allow a health specialist to enter and report on data relating to Patient, Episode, Pathway and Services provided, and will provide integration with RedCap, the online system used for managing patient surveys.
- **RedCap server:** RedCap (Research Electronic Data Capture) allows users to build and manage online surveys and databases quickly and securely. REDCap is used in numerous projects all around the world. We will use RedCap to securely manage and serve forms to be filled online by patients or health professionals.

The following diagram explains how the components of the Data Collection system work together:



Minimum Requirements and Installation Scenarios

The Data Collection system will be a desktop application installed on site at hospitals. It will be written using the industry standard Microsoft.NET platform. This means that it will be written and tested to work on any Windows PC running Windows XP or Windows 7. There will be a few pre-requisites which need to be installed (for example, Microsoft .NET Framework Version 4).

The system will use the industry standard Microsoft SQL Server as a database back-end for the desktop application. If the client site already has a SQL Server this can be used, otherwise SQL Server Express can be used – this is a free version of MS SQL Server that allows up to 5 machines to connect to a database. The supported version of SQL Server will be 2008 R2.

Minimum Hardware and Software Requirements for Client Machines

- **Operating System:** Windows XP or Windows 7
- **RAM:** 2gb
- **Processor:** no specific requirement
- **Minimum Screen Resolution:** 1024 x 768

Supported Installation Scenarios

We will support 3 possible scenarios for installation:

- 1. The installation site does not have a SQL Server, and only a single machine needs access to the application.**
SQL Server Express will be installed on the client machine.
The application will be installed on the client machine and configured to use the SQL Server Express instance on the client machine.
This will require no special network or firewall configuration.
- 2. The installation site does not have a SQL Server, and more than one machine needs access to the application.**
SQL Server Express will be installed on one of the client machines, or on an existing hospital server, as deemed appropriate by hospital IT policy.
The application will be installed on desktop machines and configured to use the SQL Server Express instance on the client machine or server on which it is installed.
This will require the SQL Server port to be opened on the client machine or server on which the SQL Server Express instance is installed.
- 3. The installation site already has a SQL Server.**
The database can be hosted on the existing SQL Server, with security configured to the satisfaction of hospital IT policy.
The application will be installed on desktop machines and configured to use the existing SQL Server as the common database.
This will require the SQL Server to be directly accessible to client machines. If that is a problem for security policy, please see options 1 and 2.

RedCap

The RedCap server will be hosted by University of Wollongong in a secure server room. The processes proposed in this document mean that while surveys will be conducted using this server, no identifiable data will ever be housed on this server.

No installation will be required on site for use of this survey system. A lightweight internet connection will be required in order to allow the desktop application to initiate surveys, and to pull the survey response data back from the RedCap server. Both of these processes will be automated from the desktop application so the user will never have to actually use the REDCap server directly. The server will have to be whitelisted if the hospital has such a

policy. All data sent to and from the REDCap server will be transmitted via a properly certified secure (SSL) connection.

System Installation and Configuration

Two installers will be provided:

- Pre-requisites installers
- Desktop Application Installer (which will install a lightweight version of SQL Server Express if option above is used).

Please refer to the previous sections (Installation Options and Minimum Requirements) for the 3 supported installation configurations.

Installation

Installation will involve 3 main steps:

1. Installation of SQL Server Express on one machine (only necessary for options 1 and 2)
2. Installation of pre-requisites (.NET Framework, Crystal Reports Runtime and its dependencies)
3. Installation of the epiCentre Application

Configuration

1. Creation and configuration of the SQL Server Database. There are two options here and more detail will be provided in the next section:
 - a. The Desktop Application will contain a '**database configuration wizard**' which will allow setup of a database connection and creation and configuration of the database via an 'SQL Create Database' script.
 - b. We can provide an 'SQL Create Database' script for IT staff in the hospital to run directly on an existing SQL Server.
2. Configuration of the Desktop Application via a '**client connection wizard**'.
 - a. Setting up the application's connection to the database.

AHSRI technical staff will be available to assist hospital technical staff with installation.

Further Details about Configuration

Creation of the SQL Server Database

As already mentioned, the database will be created and configured using a 'create database script'.

Creating the database using the application's 'Database Configuration Wizard'

The 'database configuration wizard' in the application will ask for the following details:

- the name of the SQL Server
- details of a System Administrator SQL login which can be used for running the create database script (these details are not stored)
- the name of the database you want to create
- login and password details for the database

This script will create the Database and SQL Server logins which the database requires, and populate the database with structural records.

Creating the database in SQL Server directly using the Create Database script

If preferred, we can provide hospital IT staff with the SQL Create Database script for their review and execution directly on an SQL Server via SQL Server Management Studio.

In this case, the SQL Script will contain default passwords for 'eppoc_user' and 'eppoc_admin' which will need to be modified before execution of the script.

Configuration of the SQL Server Database

As already mentioned, some initial details will be configured in the database via the '**database configure wizard**' in the desktop application.

The wizard will then prompt for the following details:

- a user name and password for a user with the 'administrator' role:
 - o See the next section 'Security Model' for further details
- facility details
 - o name and identifier for the facility
 - o tokens for enabling secure communication between your Facility and RedCap

The 'administrator' user will have the ability to create other user accounts via user management in the application, and to update the REDCap configuration. REDCap requires API keys to allow remote creation of the surveys and pulling back of survey response data. This ensures that survey data entered by patients for one hospital will be secured to that hospital.

The data entered in the '**database configure wizard**' will be stored in the database and only needs to be entered once.

Configuration of the Desktop Application's Database Connection

For each installation of the desktop application, the database connection will need to be configured. The **client configuration wizard** will prompt for the following information:

- the name of the SQL Server and database
- SQL login details for the SQL Server
- proxy server details for sites which use a proxy server for external web communication

These details will be stored encrypted in a configuration file on the client machine. An alternative to running the **client configuration wizard** is to deploy the settings file generated on one client machine to the other client machines.

Security Model

SQL Server Security

The SQL Server database will use three SQL Server logins:

- eppoc_reader: will have the role db_datareader
- eppoc_user: will have the role db_datareader, db_datawriter
- eppoc_dbo: will have the role dbo

As already mentioned the passwords will be set for these logins in the 'create database script' so the hospital can apply their own policy to passwords and at no time will AHSRI staff have any knowledge of how to access the SQL Server database directly. The 'database configuration wizard' will therefore need to request those passwords once.

Any identifiable data collected by the system will be stored encrypted in the database, using an encryption key provided during the database configuration wizard.

Application Layer Security

After initial configuration, the system will require a user name and password for any user to access.

There are 4 possible user roles.

- **Administrator:** this role will give a user complete access to the epiCentre system. This includes the ability to create, modify and delete facilities, users and ePPOC data. A user with the role 'Administrator' will also have the ability to apply updates to the database structure as they are released.
- **Manager:** this role will give a user the ability to manage users (i.e. create, modify and delete). A user with the role 'manager' will have all the permissions of lower roles.
- **User:** this role will give a user the ability to use the system for data entry, retrieval and reporting.
- **Reader:** this role will give a user to read the data in epiCentre, but not to modify it.

The user details will be stored in the database, and the passwords for users will be encrypted.

Application Update Model

If updates are required to the system, these will be provided via a Windows Installer. The installer will need to be run on each client machine, and may require administrator privileges to run.

If updates are required to the database structure, the updated application will include a '**database update wizard**'. This will only be executable by a user with the 'administrator' role. The database update wizard will connect to the database using the 'eppoc_admin' user and execute an 'Update Database script'. Alternatively, AHSRI can provide hospital IT staff with the Update Database script to execute directly on their SQL Server.

Firewall / Whitelisting Requirements

Client to Database Server

If you are using Installation scenario 1 (SQL Server and application installed on a single machine), there are no requirements for firewall between client and database server machines.

For the other scenarios the SQL Server TCP/IP port will need to be open on the machine running SQL Server. In a standard installation this is port 1433.

Client to REDCap Server

The REDCap server will have the following URL: <https://eppoc.ahsri.uow.edu.au>

This server will need to be whitelisted in firewalls. As previously mentioned, running on HTTPS means that any data to and from the REDCap server will be encrypted. Additionally, no identifiable data will be collected by the surveys run through the REDCap server.

Data Storage Requirements

A data dictionary can be provided on request, however it has more detail than is required for this overview document. The data storage requirements for the database are minimal as almost all data collected is small text fields or numerical items.

Here is a brief summary of the data tables, estimated number of records and size of each record.

Table	Records Per Patient	Size per Record	Est. Storage per Patient
Patient	1	1 kb	1 kb
Episode	3	100 bytes	0.3 kb
Pathway	3 (per episode) = 9	100 bytes	0.9 kb
Occasion of Service	200 (per episode) = 600	100 bytes	60 kb
Survey	27	1 kb	27 kb
Total			~ 100 kb

Over the 6 to 9 months of Phase 1 of the project we in fact only estimate to have 1 episode per patient, so these figures are pessimistic in terms of storage requirements.

Allowing an overhead of 10mb, for a database of 1000 patients we would expect the database to use a capacity of:

Item	Per Unit	Number of Units	Storage Required
Overhead	3mb	1	10 mb
Patient Data	100kb	1000	10 mb
Total			20 mb