Title	**The Ottawa Methods Centre EDCS Design & Development**
SOP Code	SOP02_2014
No. of Pages	14
Effective Date	01-Feb-2014

1.0 PURPOSE

This Standard Operating Procedure (SOP) describes the Ottawa Methods Centre (OMC)'s data management processes as they pertain to the design and development of web-based Electronic Data Capture Systems (EDCS) by OMC's Data Management Services.

2.0 SCOPE

This SOP applies to the design, data collection set-up, test, validation, implementation, maintenance, and support functions for the EDCS. It outlines the responsibilities of the DMS team as they pertain to the above-mentioned components of the SOP as well as related responsibilities of research study personnel in complying with the procedures set out by OMC. This SOP is applicable to all regulated and nonregulated clinical trials

3.0 REFERENCES

3.1. APPLICABLE REGULATIONS AND GUIDELINES

U.S. Department of Health and Human Services, Food and Drug Administration, July 2018, Guidance for Industry, Computerized Systems used in Clinical Investigation, Office of the Commissioner (OC). Web Link:
https://www.fda.gov/media/97567/download
https://www.fda.gov/media/94040/download

Health Canada: Regulations amending the food and drug regulations:
http://www.hc-sc.gc.ca/dhp-mps/compli-conform/clini-pract-prat/reg/1024_tc-tm-eng.php

Tri-Council Policy Statement: TCPS 2nd edition: Ethical Conduct for Research Involving Humans.
Web Link: http://pre.ethics.gc.ca/eng/tcps2-eptc2_2018_chapter2-chapitre2.html

3.2. REFERENCES TO OTHER ACTs

Ontario Personal Health Information Protection Act (PHIPA), 2004, S.O. 2004, c. 3, Sched.A https://www.ontario.ca/laws/statute/04p03/v29

3.3. REFERENCES TO OTHER SOPs

OMC-DMS SOP01_2014

4.0 DEFINITIONS

OMC	Ottawa Methods Centre
DMS	Data Management Services
ECDS	Electronic Data Capture System
SCT	Study Coordinating Team
PI	Principal Investigator
CCT	Central Coordinating Team

5.0 RESPONSIBILITIES

5.1. Data Management Services (DMS)

OMC-DMS designs, codes, tests, implements, and maintains of the thin-client web-based EDCS. DMS full list of responsibilities include:

- Design, code, and modify the EDCS as per CCT's specification and requests
- Test code and/or data modifications prior to submission to the CCT for final acceptance testing and validation checks
- Provide EDCS information upon request
- Provide user support throughout the EDCS system life cycle, including trouble shooting

5.2. Study Central Coordinating Team (Study CCT)

The study CCT responsibilities is to provide the Ottawa Methods Centre Data Management Services (OMC-DMS) team with the **final** paper Case Report Forms (CRFs), make all required changes and modifications in a timely manner, and carry-out EDCS final validation checks and perform acceptance testing before any EDCS release into 'live' mode. The study CCT coordinates the selection of study users, activates sites, maintains master user lists and provides study site users with proper training and all necessary information regarding the usage of web-based EDCS. In addition, the study CCT and the study monitoring teams must regularly check the data in the EDCS and perform data quality control. Their responsibilities are to ensure that all users of the system are adequately trained, entered correct data, and assigned with proper user role, either blinded or un-blinded.

5.3. Clinical Sites

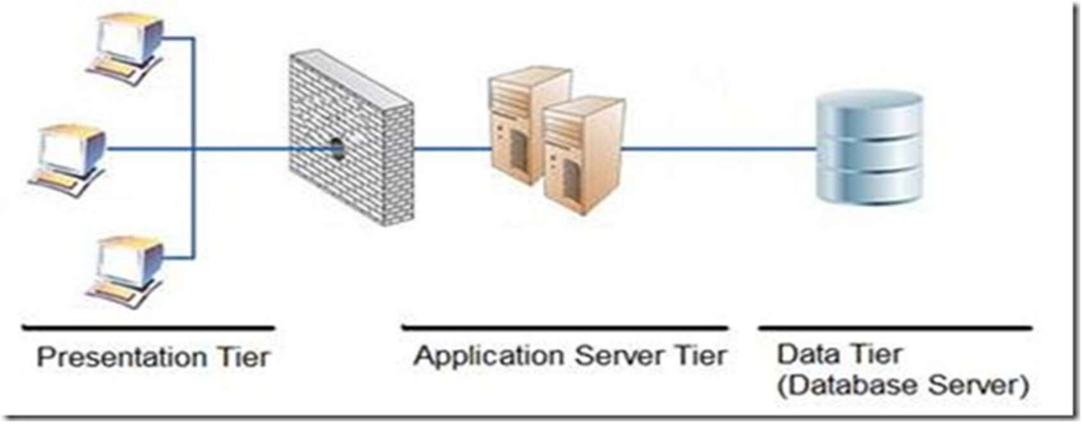
The site users are responsible for collecting study data, verifying and entering site participant data into the web based EDCS properly, correctly, and timely. The site coordinators are also responsible for verifying data after entering data into the EDCS and to respond to any queries from the study CCT. The site coordinators are responsible for notifying the study CCT if there are any staff changes, any new site user, and any issue with the EDCS. The study CCT will review and relay the messages to the OMC-DMS team.

6.0 ELECTRONIC DATA CAPTURE SYSTEM (EDCS) PROCEDURES

All EDCS development is based on the Electronic Data Management Plan (E-DMP) for each study. The E-DMP outlines the procedure of creating the web-based EDCS, based on the OMC-DMS platform, from initial paper CRFs. The paper CRFs are first developed and approved by the study PI/CCT and approved by the local REB(s). The study CCT sends the final CRFs to the OMC-DMS team for designing, coding, testing, validating, implementing, and maintaining the web-based EDCS. All subsequent changes and modifications to the final CRFs must be approved by the PI and the REB(s) before the CCT sends it to the OMC-DMS for modifications, testing, validating and implementation. Subsequent user guides are developed by the study central coordinator.

6.1. System Description

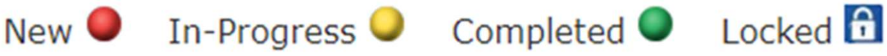
The OMC-DMS EDCS is a thin-client 3-tier web-based application as shown below.



The **Presentation tier** is responsible for communication with the users and uses objects from the Application tier to respond to the user graphical interface raised events.
The "Presentation Tier" is the client, or the site users. The users, typically study coordinators at the study sites (RAs/RCs), access the web-based EDCS application online by using any of the four (4) supported internet web browsers: MS Internet Explorer, Firefox, Safari and Google Chrome. The site coordinator/user is provided with a unique

login account to access to the EDCS. Each study's EDCS is on the internet in the TOH DMZ behind a firewall (DMZ stands for demilitarized zone and is a perimeter network that protects an organization's internal local-area network (LAN) from untrusted traffic)). All users are authenticated by logging into a unique web URL (provided by OMC-DMS) and enter participant data into web forms/pages.

The web based EDCS allows site users to enter all data on the paper CRFs (or from electronic records) into the web forms easily. All data is electronically validated based on the edit check rules that are set by the study CCT. Every web-based form has four statuses: new (red), in-progress (yellow), complete(green), and lock (lock image). The "new" status is auto-set when the web form is completely empty, i.e. blank form; the "in-progress" status is set when the web form is partially filled; the "complete" status is set when the form is completely filled with no missing data or the site user sets it to complete. It is set to lock once the data is reviewed by the monitors.



New 🔴 In-Progress 🟡 Completed 🟢 Locked 🔒

The **Application server /web tier** logic functionality is broken into three parts:

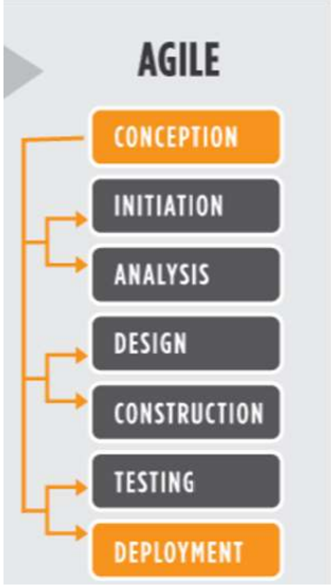
- Obtain and send data to the database tier.
- Obtain and receive data from the presentation tier.
- Perform necessary calculations and/or data manipulations.

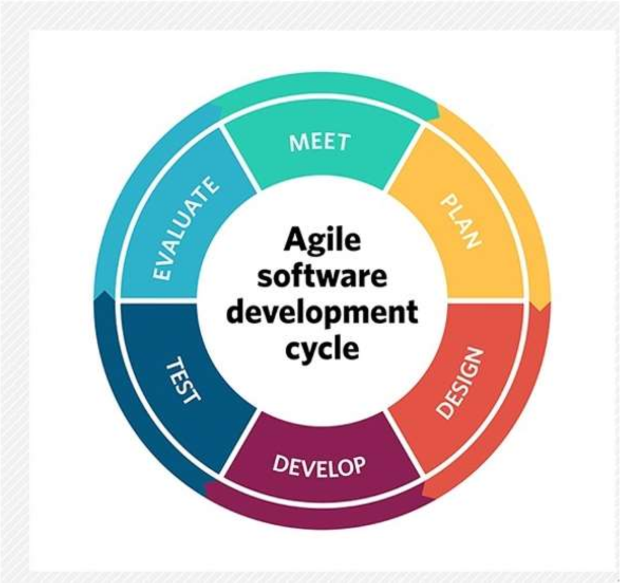
In the OMC-DMS application, this tier consists of the Application tier and Data Access sub tiers. The Data Access sub tiers are responsible for establishing a database connection.

The **Data tier** encompasses the database. The database is designed and configured using a validated MS SQL Server. The MS SQL supports the LINQ & ADO.NET dataset, which is a memory-resident representation of data that provides a consistent relational programming model regardless of the source of data it contains. A dataset represents a complete set of data including the tables that contain, order, and constrain the data, as well as the relationships between the tables.

6.2. Software Component

OMC-DMS' software development plan for web based EDCS entails Agile Methodology. The development plan makes use of user requests to plan a release, with the requests being handled in an iterative manner to accommodate changes to user requests, problems, etc. Agile Methodology allows small releases of the software to be put in the production environment once a set of acceptance tests have been conducted.





6.3. System Setup, Maintenance and Security

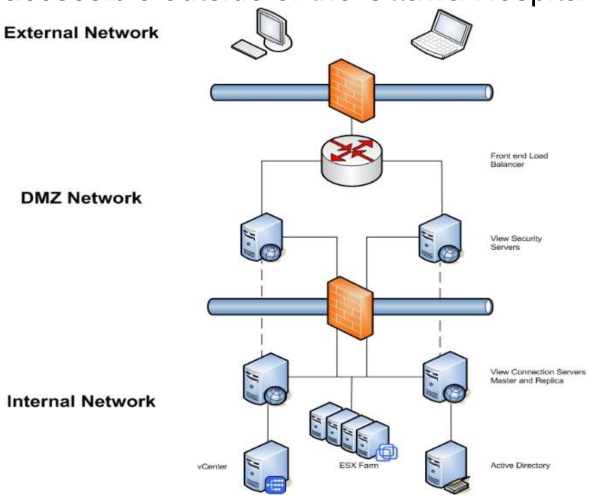
The OMC-DMS EDCS is a web application custom developed for each study by web developers at the OMC-DMS. The system is specifically designed for the purpose of securely collecting data for purposes of clinical research studies. The OMC-DMS EDCS is designed, coded, tested, validated, implemented and maintained using the following software packages: MS Visual Studio (VB.NET/ASP.NET), CSS, HTML, LINQ and JQuery (For presentation and application layers) and the back-end database is designed and implemented using Microsoft SQL Server technology. MS Visual Studio package is a complete set of development tools for building secure web sites, ASP.NET web applications, XML Web Services, desktop applications, and mobile applications. It provides a much simpler and faster way to create Web Forms pages and Web applications through Web site project or ASP.NET/VB.NET.

N-tier data applications are applications that access data and are separated into multiple logical layers, or *tiers*. Separating application components into discrete tiers increases the maintainability and scalability of the application. It does this by enabling easier adoption of new technologies that can be applied to a single tier without requiring you to redesign the whole solution. N-tier architecture includes a presentation tier, a middle-tier, and a data tier. The middle tier typically includes a data access layer, a business logic layer, and shared components such as authentication and validation. The data tier includes a relational database. N-tier applications usually store sensitive information in the data access layer of the middle-tier to maintain isolation from end users who access the presentation tier.

The OMC-DMS web developers work from their own workstations and the project/website codes are located on a secured network shared drive using a source version control package: Subversion (SVN) and integrated with MS Visual Studio package using AkhSVN. Backup of the development software codes is done on the OHRI server (network drive mapping) on a regular daily basis. The secured network drive is backed up by a daily automated software backup that is provided by the OHRI-IT server team.

Prior to the release of any EDCS to the production environment, it must pass a set of internal tests (developer and DMS staff independent tester, study CCT acceptance and validation tests). Once completed, it is to be uploaded using SFTP protocol to the production server upon approval from the study CCT.

The OMC-DMS web and database server is physically located in a secured environment behind locked doors in the TOH data centre which is accessible by a limited list of authorized personnel (TOH IT server group). The web and database server are securely protected virtually in the DMZ behind a firewall. The server is loaded with Windows Server, MS SQL Server with all the latest services patches and always has the most up-to-date virus and spyware updates. Any OMC-DMS web application is an internal network application. Hence, it is not searchable by Google or Yahoo/Bing and is not accessible outside of the Ottawa Hospital network.



6.4. Development System and Production Server

The OMC-DMS developer systems are configured with Windows 10, Office 365, MS Visual Studio and SQL Server. All development work is tested in design mode on the local systems before it is uploaded to the secured study site folder. Once it is tested and approved by the study CCT, it is transferred by FTP to the production site and is re-tested. The production web server is configured with Windows 2008 R2 Server OS, MS SQL 2008 R2 Server and only 1 port is open for FTP file transfer. All other ports are closed for security reasons.

Passwords are encrypted at the time of transmission over the Internet. The encryption mechanism is using .NET encryption cryptography. Data transmitted over the Intranet during reads or updates of records are not encrypted. The data transmitted contains no identifying information. If someone tries to access the application at a specific page without properly logging in, such as going directly to the screening form, the web based EDCS will redirect the user to the login page. Testing of the redirection is performed on all pages.

6.5. Securing the Network and the Host

The EDCS for any study is hosted on a physical server (not in the Cloud) that is located at The Ottawa Hospital (TOH) data centre in a secure server room with access limited to authorized personnel. The web/database server is behind the TOH firewalls, it is in TOH's DMZ. The OMC web server is secured with the highest rating from Entrust SSL virtual test. Data transfer between client and server is protected with Entrust SSL 2048-bit encryption. All data transfers between the client computers/browsers and the server/database are encrypted. Other tools that are used to ensure a secure network are as follows:

- Up-to-date anti-virus and anti-spyware software is installed on servers and PCs.
- Firewalls and proxy servers are used.
- The latest security patches from Microsoft and other vendors are installed.
- Mandatory password length and strong encryption.
- Encrypted password during network transmission.
- Role-based security to limit user's access.
- Server-side code is used instead of client-side code for performing validation.
- Database query is made through database stored procedure instead of embedding SQL statement inside application.
- Mandatory session timeout when the application is inactive for a given period.
- All data transfer between client system and server is encrypted with SSL 2048-bit

6.5.1. Access

For any OMC-DMS developed EDCS, each study site user is provided with a unique account, i.e. username and password. This required the relevant study CCT to provide the OMC – DMS team with a list of participating sites and contact information. OMC-DMS adheres to the United States Food and Drug Administration (FDA) 21 CFR Part 11 Regulation11.10(d) recommendation of only one unique individual account per user.

Every user account has profiles that define:

- Which site they belong to.
- Which role they belong to.
- Which type of information (forms) they can have access to.
- Activation date /De-Activation date

Accounts are used to login into the system. Once the web-based eCRF elements are completed, users must log-out of the system using the logout option. At any time, users can log back in to update participant information.

The system does not limit the number of logins, as update capabilities are permitted. Built-in audit trails capture the changes made to the data previously saved. At present, the system does not limit the number of logins after several unsuccessful attempts.

When users finish using the system, they have to logout. In the event users do not logout, an automatic logout of the system occurs after a predetermined time period (typically 30 minutes of idle time). Users need to save their data at the question level to ensure that the timeout does not kick them out the application without saving their work.

External access to the web system is done using a web browser. A computer with a web browser can access the study by typing a study specific, OMC-DMS issued web URL. This web link is an OHRI-DMS intranet sub-domain and it is internal to TOH's network.

6.5.2. User Adherence to Security Measures

OMC-DMS requires responsibility from every site user to:

- Keep user account information secret.
- Only log in when user needs to access the EDCS.
- Log off after using the system or auto-log off feature will activate.
- Ensure the computer system is not accessible by any other unauthorized user.
- If the site user prints a page, the user should follow all procedures in place to maintain the confidentiality of the information for the enrolled participant.

After a period of inactivity on the web-based system, the system will automatically log off the user from the application.

6.6. DATABASE SETUP, MAINTENANCE AND MANAGEMENT

The OMC-DMS completes all database set up using MS SQL Server with 3rd normal form. OMC-DMS uses database normalization as the process of organizing the fields and tables of a relational database to minimize redundancy and dependency. This usually involves dividing large tables into smaller (and less redundant) tables and defining relationships between them. The objective is to isolate data so that additions, deletions, and modifications of a field are made in just one table and then propagated through the rest of the database via the defined relationships. Any time there is a change to the database (table, field, type, etc.), a full database backup is done. A data definition file or metafile is prepared by the DMS developer and is updated regularly.

The database is backed up daily at midnight by auto-backup software and is managed by OHRI-IT staff. It is also routinely backed up to a remote location (off-site) on a weekly basis. Database extraction for data validation, DSMB review, and preliminary analysis has to be requested formally (in writing) by the study CCT team. The database can be extracted to MS Excel or CSV format and is encrypted if it is sent by email. Database security: a limited number of authorized users have access to the study database and is listed below:

- TOH IT Server Staff
- OMC-DMS web developer
- OMC-DMS Manager

The study database developer is a staff at the OMC–DMS who manages all database activities: i.e. design, code, test, and support and maintenance

6.7. SYSTEM BACKUP AND CONTINGENCY PLANS

DMS-OMC collaborated with TOH IT. TOH's IT server team is responsible for SQL database backup, security patches, and equipment replacement. In conjunction with the OMC-DMS team, planned downtime is assessed and users are notified of the system unavailability. Appropriate backup of the system is made prior to changes on the system and users are notified when the system is back online.

System back up and archiving are done using services provided by TOH IT Server team. TOH IT server team ensures that:

- The OMC-DMS web server is on uninterrupted power in the data centre.
- The OMC-DMS web server is in a TOH secured zone and behind firewalls.
- Physical location for the server in the data centre is protected by locked doors.
- Only limited authorized personnel are granted access to the web server.
- The server is backed up nightly on-site and weekly off-site. The contingency plan includes a system restore from high capacity tape backup.
- The server is backed-up daily with a proper back-up system following TOH IT procedures.

In the event the an EDCS is unavailable, users of the system are to contact the OMC DMS support staff. The OMC-DMS staff will investigate the issue. Alternative methods of recording the data are to first use a paper CRF and then enter the data electronically when the web application server is back up and running.

6.8. SYSTEM VALIDATION

OMC-DMS Standard

OMC-DMS aligns its procedures with the principles of the **FDA's 21 CFR Part 11 Regulation** (enacted in 1997) which outlines criteria for acceptance by the FDA for electronic records, electronic signatures and handwritten signatures. With this regulation, titled Rule 21 CFR Part 11, electronic records can be equivalent to paper records and handwritten signatures.

Requirements of Part 11 are:

- Use of validated existing and new computerized systems.
- Secure retention of electronic records and instant retrieval.
- User-independent computer-generated time-stamped audit trails.
- System and data security, data integrity and confidentiality through limited authorized access to systems and records.
- Use of secure electronic signatures for closed and open systems.
- Use of operational checks.
- Determination that the persons who develop, maintain or use electronic systems have the education, training and experience to perform their assigned task.

6.8.1. Systems Validation

OMC-DMS server operating system (MS Windows Server OS) and MS SQL Server software are installed, configured and validated by both TOH-IT staff and OHRI-IT staff. This web and database server ensure accuracy, reliability, consistency with respect to the intended performances, and the ability to discern invalid or altered behavior. The web server and database server hardware is made by HP vendor, proven to be one of the industry's most reliable systems.

The DMS developer system is provided and configured by TOH/OHRI-IT clinical standards. It has Windows 10 Pro OS, MS Visual Studio, MS SQL Server Management Express, MS Office 365, Anti-Virus, Anti-Spyware (McAfee), FileZilla FTP, MS IE, Firefox and Chrome browsers, and Sub-version Version Control installed.

6.8.2. EDCS Validation Procedure

The OMC-DMS validation procedure is covered by **SOP01_2014**.

6.8.3. EDCS Audit Trail

The OMC-DMS EDCS is developed with procedures to generate secure, computer-generated, time-stamped audit trails to independently record the date and time of site user entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation is retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying. The database also scripted with a full audit trail which all changes to all data fields are also tracked and dated in the SQL database. Data history of any data field can be generated from the database.

All the system's date and time is provided by the web server where the EDCS production source codes reside. Therefore, date and time are not dependent of the end user workstation's settings. There are no anticipated date and time changes, other than changes to adjust to daylight savings time. Dates are provided following the standards, such as DD/MMM/YYYY. Time is displayed as the 24-hour clock format.

The ET (Eastern Time) will be used throughout the system as the time is picked up from the server located in Ottawa, Ontario. When date/time stamps are computer generated, the date and times are read from the web server. Users can enter date and times using three distinct drop-down lists to select day, month and year. As for randomization date and time stamp, it is the user local time that is to be recorded in the system, not the server time. The local user time is pre-set in the user table in the database. Upon successful login, the system determines the local user time.

6.9. RISK MANAGEMENT

OMC-DMS has identified 2 types of risks, physical and virtual risks. Physical risks such as fire and water damage to the secured server room, web server hardware failure, damage and/or malfunctioning, etc. have been evaluated. Risks are mitigated with on-site and off-site back-up of the server data by TOH Information Technology (IT) server team to prevent data loss in a worst-case scenario. Server hardware and spare parts are available on site. TOH's IT server team is available 24/7. Virtual risks such as hacking, DoS, spyware and virus, loss of internet connectivity, etc. have also been reviewed. They are mitigated through TOH's IT server staff installing all critical patches and security updates are properly applied and provisioned in a timely manner. Server security is routinely checked and assessed by security experts.

6.10. PRIVACY

The OMC-DMS EDCS does not collect/retain any personal/protected health information (PHI). All uploaded participant forms/images/records are properly de-identified by site users. OMC-DMS flags any data and/or documents that contain PHI for removal and/or deletion upon user notification by OMC staff. The warning text below is displayed to all site users in the file uploading section.

"We will not accept any documents/files with identifiers that can be used to identify patients. Items such as patient names, address, phone and health insurance numbers, next of kin names or contact information are strictly forbidden and violate the Personal Health Information Protection Act, Ontario 2004 (PHIPA) and The Ottawa Hospital policies on privacy. Patient identifiers must be removed from any documents/files (blacked out, covered with stickers, etc.) prior to scanning and uploading to the website. All items received containing identifiers will be deleted automatically upon notification and a request will be sent asking for the documents to be deidentified and re-uploaded"

6.11. CHANGE CONTROL

6.11.1. Software upgrades, change of code

There are times when OMC-DMS actions software upgrades and/or change of codes are required in the production environment. In this case, a prior communication is sent to all users, affected departments and sites, OHRI IT and TOH IT to indicate that the application will be unavailable on the day/time of the upgrade. The OMC-DMS may wish to indicate the reasons for the change to the user community. A full system testing has occurred prior to the upgrade taking place. Backups of the production systems are done each night and the upgrade will be conducted whenever the new system is ready. Typically, the upgrade is completed first thing in the morning before any changes are made to the data, so that if a restore from the backup is required, the restore will have the most up-to-date data.

The OMC-DMS requests the participation of the OHRI IT or TOH IT for hardware/software configuration or any other tasks requiring their participation as needed. When OHRI IT or TOH IT are involved, they are contacted few days in advance to ensure that the upgrade is completed on time. Once the changes to the application are made, a high-level test of the application is completed to ensure that it is working as expected before handing it back to the users.

If there are database changes (i.e., changes to the database tables as part of the upgrade), OMC-DMS completed a validation to ensure that the data is clean and accurate following the upgrade. This could include running a standard report or a standard query before and after the upgrade to compare the results, identifying a number of records in each of the tables before and after the upgrade and compare the results. OMC-DMS manages any issues, problems or performance with the application following the upgrade.

The OMC-DMS assumes responsibility of user training that is required due to the changes of the application with the application main coordinating site. In the event there are any problems with the application following the upgrade, the OMC-DMS coordinates with OHRI IT or TOH IT for assistance with a restore from the saved backup. A request is made and assistance is part of the change management. Users are notified that the downtime may exceed the planned outage and are made aware of issues, if any. Once the upgrade is complete and testing confirms the availability of the application, users are notified that they can resume their activities on the system.

6.11.2. Security Patches and Equipment Replacement

TOH/OHRI IT is responsible for security patches and equipment replacement. In conjunction with the OMC-DMS, planned downtime is assessed and users are notified of the system's unavailability. Appropriate backup of the system is made prior to changes on the system and users are notified when the system is back online.

6.11.3. Training

Training of site end-users is done by the study CCT. Site users are also provided with a test account that they can use to test and to learn the system. When changes are made to the system, users can get familiarized with the changes using a test account or their real account as long as they don't save data while in learning mode. The study user guide is developed by the study CCT and available to all site users.

6.11.4. EDCS Site and User Activation

Site Activation

1. Study CCT sends request to OMC-DMS to add new site and/or new user info by updating the Master User List file. Highlight new changes, email to DMS.
2. OMC-DMS acts upon request and sends email confirmation once it is activated.
3. OMC-DMS updates the Master User List file with activation/start date.

User Account Activation

1. Study CCT sends request to DMS to add new users that includes
   - User full name, User email, and User role
   - User site id, Notification Email (Yes/No), Special Access
   - Study CCT updates Master User List log file, sends it to OMC-DMS
2. DMS activates the account and sends an email confirmation to the CCT team.
3. DMS sends the new account information to the user.
4. DMS sends a confirmation email to Study CCT to confirm account activation

User Account De-Activation and Re-Activation

1. Study CCT sends request to DMS for user De-Activation, required info:
   - User full name, User email, User role, User ID, deactivation date
2. DMS de-activates the account and sends an email confirmation to the study CCT.
3. Study CCT updates Master User List log file with de-activation date.

Password Resets:

1. Site Users are required to change their password every 24 months in order to continue having access.
2. In case site user forgets his/her password, site user can request a new temporary password by clicking on a “Reset Password” button. The user is prompted to enter his/her username and email, both fields are case sensitive. If the credentials match the information in the Master User list, a new password is emailed to the user.

OMC-DMS does take any phone request from any site user to reset a password.

6.11.5. Source Documentation and Retention

The data collection requirements will vary by study and collected data will be entered into an EDCS by site study staff. Data that is collected on paper first (i.e. questionnaires) will be entered into the EDCS and the hard-copy source document will be signed and dated and filed in the participant's study file. Data from the patient's medical charts is entered directly into a study's EDCS. The e-data resides in the study's respective MS SQL database. Data will be stored in the study's MS SQL Database for 2 years following study completion. For uploaded files (study & participant files), OMC-DMS provides the study team with a shared folder location where they can copy all needed files and transfer them into their own network shared folder Subsequently, the final dataset will be provided to the study PI by email in Excel file format.

6.11.6. System Support

EDCS system support is provided by OMC-DMS by phone and email. User experiencing issues or concerns are instructed to contact OMC-DMS as follows:

8:30am to 4:30am (ET)
By Phone: 1-613-737-8899 Ext.73804 (Dong Vo)

By Email: dms@ohri.ca

Web server and database server support is provided by the TOH-IT server group and OMC-DMS liaises with them as needed 24/7.

7.0 REVISION HISTORY

SOP Code	Effective Date	Pages	Revision
SOP02_2014	Feb-2014	5	Original version