Deliverable No. 9.3

Report on the validation and certification of ObTiMA and DoctorEye

Grant Agreement No.:	270089
Deliverable No.:	D9.3
Deliverable Name:	Report on the validation and certification of ObTiMA and DoctorEye
Contractual Submission Date:	31/07/2012
Actual Submission Date:	31/07/2012

Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

COVER AND CONTROL PAGE OF DOCUMENT	
Project Acronym:	***p-medicine***
Project Full Name:	From data sharing and integration via VPH models to personalized medicine
Deliverable No.:	D 9.3
Document name:	Report on the validation and certification of ObTiMA and DoctorEye
Nature (R, P, D, O)[1]	R
Dissemination Level (PU, PP, RE, CO)[2]	PU
Version:	1
Actual Submission Date:	31/07/2012
Editor: Institution: E-Mail:	Holger Stenzhorn USAAR holger.stenzhorn@uks.eu

ABSTRACT:

This deliverable presents an overview both of the necessary requirements to validate and certify ObTiMA and DoctorEye as well as of the current state of fulfilling those requirements.

KEYWORD LIST: validation, certification, ObTiMA, DoctorEye

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 270089.

[1] **R**=Report, **P**=Prototype, **D**=Demonstrator, **O**=Other

[2] **PU**=Public, **PP**=Restricted to other programme participants (including the Commission Services), **RE**=Restricted to a group specified by the consortium (including the Commission Services), **CO**=Confidential, only for members of the consortium (including the Commission Services)

MODIFICATION CONTROL			
Version	Date	Status	Author
0.1	02/07/2012	Draft	Holger Stenzhorn
0.2	13/07/2012	Draft	Holger Stenzhorn
1.0	31/07/2012	Final	Holger Stenzhorn

List of contributors

- Holger Stenzhorn, USAAR
- Ruslan David, USAAR
- Wolfgang Kuchinke, UDUS

Contents

1 Executive Summary

This is the initial iteration of the report on how the validation and certification should be planned and performed within the scope of the ObTiMA and DoctorEye applications.

In this version of the report we describe the foundational basis for all of the validation and certification procedures through a collection of standardized, regulatory criteria that must be necessarily fulfilled in order to pass the procedures successfully.

More specifically, we present

- a System Validation Master Plan (SVMP),
- the key requirements according to CDISC and EU GCP Inspectors Working Group,
- the standard requirements for GCP-compliant data management in multinational clinical trials,
- the requirements of the FDA Title 21 CFR Part 11 and
- the FDA industry guidance.

To conclude we provide an initial estimation about the overall applicability of the presented criteria for ObTiMA and DoctorEye.

2 Introduction

According to the description of work of p-medicine, all tools that are being developed within the frame of that project and which are intended to be used in GCP-compliant trials are subject to undergo a validation and certification process. In collaboration with the other work packages 2, 6, 8 and 15, a concrete plan and methodology for this validation and certification is to be specified within task 9.3.

The expected goals are to validate and/or certify ObTiMA and DoctorEye platforms since those applications will be directly employed within the scope of GCP-conformant clinical trials. The validation and certification of other p-medicine tools and applications depends on the actual need of their conformity with the GCP criteria and will be assessed for each tool specifically over the lifetime of the project.

ObTiMA as an ontology-based trial management application will be further developed, evaluated and validated mainly within task 8.4. Also task 8.3 – taking care of data de-identification and pseudonymisation tools – is relevant because those are to be integrated in ObTiMA. This goes further in hand with task 5.1 that analyses the data protection and data security framework and sets up of this framework.

DoctorEye as an integrated platform will serve as a powerful clinical tool to perform in-silico clinical trials on cancer allowing clinical users the analysis and segmentation of DICOM images together with the visualization of multi-modality tomographic data, in a single user-friendly environment. Here, it offers a variety of tools and services that include cancer growth simulation, as one main task of WP12. Also, the platform provides modules for comparison of simulation results to the actual outcome for validating the predictive power of models, a task undertaken together with WP15.

2.1 Scope

It is important to stress that this report is the first iteration on how the validation and certification activities is planned and performed within the scope of the ObTiMA and DoctorEye applications.

This means that in the following we start by describing the foundational basis for all of the validation and certification procedures through a collection of standardized, regulatory criteria. Those are the criteria that must be necessarily fulfilled in order to pass the procedures of validation and certification successfully. Then we give some short introduction of what has already been done towards fulfilling those goals in the realm of both the ObTiMA and DoctorEye applications.

We are aware that there exists some considerable overlap between the various criteria stemming from the different sources. But our intention is to first gather a comprehensive overview of all the criteria that might be possibly applicable to our software. Then in a second round we are consolidating and merging those criteria into a single document that is then further be very useful in the software development process.

3 System Validation Master Plan (SVMP)

3.1 Purpose and Scope

The System Validation Master Plan (SVMP) introduces all system validation activities that are to be conducted during the life cycle of a clinical trial system and the necessary documentation at the data centre. Specifically, the SVMP defines the approach for providing documented evidence that the specific software system performs its various functions as integral part of a data centre's clinical study environment correctly, consistently, and according to the user requirements and will continue to do so in the future. This plan addresses the validation process for all components within the specific software system and provides a framework for validating this system in context of a clinical trials network. For this purpose data of specifically developed dummy trial are used. The SVMP also defines individual and group responsibilities inside the data centre for the validation tasks. Finally, it ensures that the system is implemented and maintained in a validated state.

This SVMP should be in effect for the current version of the software system and all future versions until superseded by a newer version of the SVMP.

3.2 Validation Policy Overview

3.2.1 Policy Compliance at the Data Centre

This plan is being written to comply with the following policy requirements of the data centre for validation as stated in the specific data centre's guidelines and as well as its handbook for quality management.

3.2.2 Difference between Software Verification and Validation

According to the FDA (General Principles of Software Validation, see later in this document), software verification provides objective evidence that the design outputs of a particular phase of the software development life cycle meet all of the specified requirements for that phase. Software verification looks for consistency, completeness, and correctness of the software and its supporting documentation, as it is being developed. Software testing is one of many verification activities intended to confirm that software development output meets its input requirements.

Software validation is a part of the design validation for a finished device, but is not separately defined in the Quality System regulation. It is confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled. In practice, software validation activities may occur both during, as well as at the end of the software development life cycle to ensure that all requirements have been fulfilled.

3.2.3 Validation Defined

For the data centre "Validation" denotes establishing documentary evidence that provides a high degree of assurance that the data centre computer systems will consistently produce a product or result meeting predetermined specifications, requirements and quality attributes. This evidence is presented to concerned parties to provide assurance that systems and processes as well as test methods at the data centre are under control and are repeatable.

3.2.4 Validation Philosophy

Validation is a mandatory requirement for the conduction of GCP-Studies and is thereby a way of managing the quality of data in clinical studies. There are many regulatory requirements and guidelines that apply for system validation. A list of regulatory requirements and guidelines with a classification of their importance for the system validation of computer systems should be attached.

But validation also makes good economic sense for the data centre. The benefits are realized in the following:

- Higher productivity of clinical studies
- Greater consistency of study conduct
- Fewer rejects, fewer repetitions during study conduct
- Lower utility costs
- More efficient use of software
- More effective use of human resources
- Greater confidence of everybody using the computer system for clinical studies
- Validation documents consist of highly formalized protocols, checklists, test procedures, Standard Operating Procedures (SOPs) and protocol final reports. Protocols are written, reviewed, approved, and then executed by qualified personnel at data centre using repeatable test procedures. Upon completion of tests, the results are documented, evaluated and reviewed to provide evidence that the clinical study environment, the study equipment and processes are under control and are capable of producing data and reports of clinical studies meeting the data centre's specifications and the GCP-standards.

Software validation takes place within an established software life cycle. The software life cycle contains software engineering tasks and documentation necessary to support the software validation effort. In addition, the software life cycle contains specific verification and validation tasks that are appropriate for the intended use of the software.

Notice: this SVMP is to be regarded as an active document: sections and parts should be added, deleted or modified according to the needs of the data centre. The SVMP can be linked with other documents and lists that describe in detail the necessary regulatory requirements, change control of the software, security infrastructure of computer systems and study test scripts and data.

3.2.5 Validation Programme

The achievement of a validated state of the computer system is accomplished by successful execution of a series of qualification protocols and approval of each subsequent final report. With Change Control this validated state is perpetuated.

Based on the complexity and functional requirements of a given system, one or more qualification activities are performed. Major computerized systems will require in general an Installation Qualification (IQ), an Operational Qualification (OQ) and a Performance Qualification (PQ). In addition, a system must be validated for GCP-compliance and observance of other regulatory requirements and guidelines, for the existence of an appropriate security infrastructure within the scope of clinical trials (see description of security infrastructure). A Validation Protocol (VP) will be used to manage the process of validation.

The Validation Program consists of following steps and topics the data centre validation team has to consider:

- If applicable an audit and acceptance of a qualified computer systems vendor can be conducted. This can also be a developer evaluation. The vendor selection

process/developer evaluation also considers the vendor's/developer's knowledge/compliance with GCP and quality documentation.

- Written procedures for test methods shall be established and validated where appropriate.
- Acceptance criteria shall be established and specified in each protocol.
- Any planned deviation from validation procedures outlined in the protocols must be approved in writing by all persons responsible for the initial approval of the protocol. An addendum describing the deviation and the approval by responsible persons will be attached to the protocol.
- In the course of executing a protocol, any exceptions/deviations from validation requirements must be explained. An evaluation of the impact on the integrity of the test data included in the Final Report.
- Standard Operating Procedures (SOPs) for maintenance, operation and parameterisation shall be written prior to execution of the applicable Operational Qualification protocol.
- Computers and additional equipment shall be validated prior to usage in clinical trial processes.
- Product Performance Qualification using data of a test study is the last step in the validation sequence (User Acceptance Test). It shall not be performed until computers, equipment, test methods and processes have achieved a validated state.
- A Final Report shall be written for each completed qualification/validation protocol.
- Validation will encompass the computerized system used for clinical trials as parts of a data centre's security infrastructure.
- Test data in the form of a clinical test study shall be recorded on pre-approved data collection forms.
- Once the systems has been considered validated a Change Control program will be implemented to ensure that both planned and unplanned changes are documented and revalidated if necessary.
- Maintenance and Change Control is part of the life cycle approach to validation of computer systems. Maintenance of computer-related systems will be conducted according to schedule to ensure proper function.
- During the life of the computerize systems, its operating conditions during performance of clinical trials will be reviewed on a continuous or regular, periodic basis and compared with predetermined criteria. Any deviations from the acceptable operating criteria will be investigated and appropriate action will be taken.
- The life cycle approach to validation and change management ensures that the computer system is always validated for the proper conduction of GCP-clinical studies during its entire duration of use.

3.3 Validation Plan

3.3.1 Scope of Validation

This section should define the scope of the computerized system that will be validated at the data centre. The rationale for this scope should also be provided: it should be explained if any portion of the system is excluded or if anything outside the system's definition is included.

It should be indicated for the data centre what validation activities will or will not be performed for the included components. Computerized system encompasses software, hardware, documentation and users.

Table 1: Example for definition of the scope of the validation project

Nr.	System part	Scope	Rationale for Validation
1.			
2.			
3.			
4.			
5.			
…			

The scope of validation for the specific software system includes all the following parts that are necessary for the system to operate (define all boundaries).

1. Controls system hardware and software
2. Hardware
3. Instrumentation
4. Other Systems
5. Facilities

3.3.2 Out-of-Scope

The scope of the validation efforts will encompass the functional areas of software, Quality Control, Quality Assurance, security infrastructure, change control and clinical trials process.

The purpose of a validation program for the computerize systems is to provide documented evidence that the computer systems needs are implemented properly at the data centre, are operating to design specification and that all security features are acceptable. Change Management routines secure that the validated computer system stays in a validated state for its entire life cycle.

The following computerized systems are subject to a specific degree of validation and are contained in the scope of the plan and thereby part of the validation.

Table 2: Computer Systems Included in the Validation Plan

	Computer Systems
1.	Application Server
2.	Database Server
3.	Webserver
4.	Firewall
5.	Client compute

3.4 SOP References

Validation is conducted according to SOPs. This chapter could serve as a template to place all data centre's SOPs and regulated documents which are important and relevant for conducting system validation. Several proposed examples SOPs are listed here:

- Data centre's Quality Management Handbook
- Relevant vendor/developer documentation
- SOP 1 - Quality Assurance Audit
- SOP 2 - Computer Validation Process
- SOP 3 - Structural Testing
- SOP 4 - Qualification Testing
- SOP 5 - Functional Testing

3.5 System Overview and Process Description

The System Overview and Process Description is a concise description of the computer system purpose and capabilities and the study process to which it will support. Notice: Documents with a detailed software description may be provided by the developer/vendor. The description will encompass the following parts:

- Data Centre Description: The details of the given data centre need to be expanded here. Specifically, the following has to be specified clearly:
    - Environment of software used at the data centre
    - Business scope and processes at the data centre
    - Tasks, workplaces and responsibilities at the data centre
- Concerned Scopes: For the given software system, the exact environment has to specified giving details for the following items:
    - Data capture system
    - Remote data entry system
    - Electronic transfer of data
    - Clinical database management system
    - Statistical System (or Other System)
- Short Description of Processes Supported by the Computer Systems
- Hardware
- Network (the Computer System as part of a Network)
- Software Description in General
- Specific Software Description:
    - Main Characteristics
    - Summary
    - Software Provider/Software Developer
    - Specific Software in Detail
    - Functions of the Specific Software in Detail

3.6 Software Development and IT Management

Software development and IT management/quality management are representing a concise description of the computer system, evaluation/testing and acquisition inclusive the quality management during software development. The expected (in further deliverables related to the p-medicine platform development) description should hold the following basic parts:

- Introduction

- Methods
- Demonstration of Software Solution
- Development Evaluation
- Reference Installations/Test Installations
- Final Assessment

3.7 Configuration and Implementation

Software solutions that are “Configurable Of-the-Shelf software” need extensive configuration and parameterisation before they can be used. Notice: Documents with a detailed description of software configuration and the testing of new configurations may be provided by the vendor/developer.

3.8 Configuration Management and Change Control

3.8.1 Introduction

Any changes required during structural, qualification, or functional testing will be handled via specific error resolution procedures defined in applicable test protocols. It is useful to define a SOP concerned with Change Control: the system will be considered to be under formal Change Control per SOP (Change Control) upon completion of all testing and approval of the system for production implementation.

3.8.2 System Configuration Management and Versioning Schema

For the notation of different software versions following scheme is suggested: System Versions will be represented as “version XY.Z,” where X, Y, and Z represent positions of numbers. An increase in the number in the "Z" position represents patches or bug fixes. An increase of the number in the "Y" position represents a full upgrade of the system software or other system component. An increase in the number in the "X" position represents a new release of the system, which is associated with a major software or hardware change.

Notice that documents which describe version numbering of software may be provided by the vendor or the developer.

3.8.3 Documentation Management

For the notation of validation documents/controlled documents following scheme is suggested. Validation and change control documentation will be maintained (define the location where it will be maintained in hard copy and electronic copy at the data centre). Cross-referencing between requirements, design documents, and structural and functional testing should be documented via a Traceability Matrix (TM).

Approved (with signature and date) hard copies of validation deliverables will be considered as official copies of data centre. Prior to formal approval, drafts will be versioned using a defined date (footer). In the event that a modification to a validation deliverable is required, all validation deliverables generated to that point will be evaluated for impact and, if impacted, will be updated accordingly. Validation documentation will be archived in accordance with an archiving SOP (SOP Document Archival and Retrieval). During the validation process, the handwritten signatures and initials of those personnel who are involved in validation activities will be correlated to their printed name in a Signature/Initials Correlation Sheet (Signature sheet), which will be retained together with the validation

documentation. In case of electronic versions of documents (e.g. PDF documents) a SOP about the design and validity of “Electronic Versions” of documents should be created (SOP “Electronic documents”).

3.8.4 Post-Implementation Changes

Post-implementation change control will document the purpose and descriptions of change, approvals, implementations, testing and test results (Refer to change control procedures).

3.9 Detailed Validation Scope and Approach

3.9.1 Data Management Workflow at the Data Centre

3.9.1.1 Responsibilities

There are responsibilities regarding the contribution to the clinical trials data flow for data management, trial management, and biometrics. They are described in aditional dedicated SOP or controlled documents.

3.9.1.2 Processes

An indicative scenario for the implementation of clinical trials at the data centre is the following example:

In most cases a clinical trial begins with a general research idea. The study management does the first steps to set up or complete the protocol. Legal issues like ethics have to be considered already in this early stage. Also the data management will be involved very early, although there might not yet exist a CRF.

Data management at the data centre is equipped with early drafts of the protocol/CRF to get familiar with the rationale and to develop the data management plan. We would describe the model of this process as “rapid prototyping”, in that sense that the final protocol and data management plan evolves out of a cyclic process. This process is regularly reviewed, but not yet in a formalized manner.

3.9.1.3 Organisational Structure and Organisational Constraints

In general following skills are necessary for conducting clinical studies:

- Data management
- Clinical management system
- Data entry
- Data management, CRF design
- Experience biostatistics, database management
- Experience with reporting, etc.

There may be a considerable overlap in the responsibilities of every employee at the data centre. Every employee has different tasks and may be involved in several trials.

3.9.1.4 Clinical Trial Management Practices

Following regulatory requirements must be considered: EMA, FDA, BfArM, AMG, MPG, and GCP. The following guidelines do apply.

3.9.1.5 Quality Management (QM)

The data centre may be responsible for in house auditing activities. Trial auditing is generally performed by sponsors or initiators. One of the main purposes of the data centre may be to improve the quality of clinical trials. This will be done by a tripartite approach: through enforcement of standards during all steps of the trial (esp. GCP), the making available of SOPs, guidelines and assistance and the training of investigators, study nurses and monitors.

A process description (e.g. a table) will list the main processes, as well as documents that are used at the data centre to facilitate clinical study workflow. The table should list processes according to the progression of a clinical trial: from the design of a study protocol to the final protocol and the archiving of results.

Table 3: Assumptions, Exclusions and Limitations Associated with the Validation Process of the Specific Software System(s)

System Name	Exclusions	Assumptions	Limitations
…			

3.9.2 Validation Approach

The specific software system will be validated in accordance with (SOP Computer Validation). Controls have been established throughout the system life cycle to ensure that the quality of computerized systems has been verified continuously.

The validation approach for the system will include:

- Documentation of the requirements, qualification, and software quality assurance practices for the system
- A risk-based approach is considered for each requirement
- Conducting of separate validation, qualification, and functional testing
- Verifying a controlled environment for the validated system
- Updating/creating required SOPs/controlled documents
- Conducting change control management for the system
- Ensuring that a disaster recovery and contingency plan is in place for the system
- Ensuring that qualified security infrastructure is in place
- Conducting the required training
- Preparing the validation report

If after any test phase, the acceptance criteria have not been met or if the system is deemed to be unstable by the Validation Team, the validation process may be halted and corrective action initiated.

3.9.3 GCP Criticality Assessment – Requirements

The GCP criticality assessment information related to the software system are continuously detailed. The requirements for determination of the levels for GCP criticality are including "Direct Impact, Indirect Impact, and No Impact" systems (three degree system).

- Direct Impact: System or components within the system where the operation, query, data, control, alarm, or failure will have a direct impact on data quality of GCP data.
- Indirect Impact: System or components within a system where the operation, query, data, control, alarm, or failure will not have a direct impact on data quality of GCP data. Indirect Impact systems typically support Direct Impact systems, thus indirect impact systems may have an effect on the performance or operation of a direct impact system.
- No Impact: System or component within a system where the operation, query, data, control, alarm, or failure will not have a direct or indirect impact on data quality of GCP data.

3.9.4 Standard Operating Procedures (SOPs)

SOPs play an important role for the proper conduct of the system validation process. The data centre has following list of SOPs that are used to support the validation of system, to support security infrastructure and corresponding change management. SOPs must be in an approved form (signature) prior to the start of execution of validation and qualification, and where applicable of other qualification tests.

Table 4: SOPs Example

No.	SOP title	Approved	
		Date	Name
1.			
2.			
3.			
4.			
5.			
…			

3.9.4.1 SOP Requirements

SOPs/controlled documents which include following topics will be in place at the data centre to ensure proper usage of software and hardware of the computerized systems.

- Software. Development, Operation, Maintenance, Software Vendor Audit, Change Control and Security infrastructure.

- Hardware. Operation, Maintenance, Backup, Contingency/Disaster Plans and Security Infrastructure
- Computer Systems Change Control Program (see: change management)
- Computer Systems Maintenance Program (see: Re-Qualification)
- Maintenance of Computer Systems Security Infrastructure
- Computer Systems Validation Program

3.9.4.2 SOPs for Structural Testing

Structural testing is only applicable if the entire system or part of it was programmed by the data centre. All functional and technical requirements and the detailed design specification provide the basis for structural testing. Structural testing will demonstrate that the system meets the technical requirements identified by the developers and the functional requirements identified by the users. The technical testing team will conduct structural testing in a controlled environment and in accordance with SOP “Structural Testing”, unless otherwise noted in the respective test protocol.

Notice that documents with a detailed description of structural testing may be provided by the developer.

3.9.4.3 SOPs for Qualification Testing

The Manufacturer's/Developer's recommendations and installation instructions provide the basis for qualification testing. Installation qualification is generally conducted by the software vendor/developer. The testing team conducts qualification testing in a controlled environment and in accordance with SOP “Qualification Testing”, unless otherwise noted in the respective test protocol. Qualification testing demonstrates and verifies that the system can be properly accessed and operates correctly with the technical architecture. It also confirms that the required documentation and support structure is in place.

3.9.4.4 SOPs for Functional Testing

The functional requirements specification provides the basis for the functional testing and is expected for later stages. The users will conduct functional testing in a controlled environment which represents the production environment of a clinical trial and be in accordance with SOP Functional Testing, unless otherwise noted in the respective test protocol. This test phase will include abnormal data testing (testing to ensure that the system responds as expected when abnormal patient data are entered) as well as normal data testing. Functional testing will demonstrate that all required functions are implemented and that they operate as expected. In case functional testing and performance testing is conducted together, this will include testing of patients with dummy data. It will also verify that the required documentation is in place and training conducted to facilitate proper use of the system in clinical trial.

3.9.4.5 SOPs for Performance Qualifications

The performance qualifications specification provides the basis for performance qualifications testing (expected for later stages). The users will conduct performance qualifications testing in a controlled environment that represents the clinical trial environment and be in accordance with SOP “Performance Qualifications Testing”, unless otherwise noted in the respective test protocol. In our approach, PQ is done together with the user requirements acceptance testing and represents together the System Validation. This test phase will include traceability to ensure that the system corresponds as expected to all user

requirements. See also: Traceability matrix. Functional testing and performance qualification may be treated as one unit until stated otherwise.

3.9.5 SOPs for System Maintenance

To ensure future reliable operation in the production environment, SOPs will be in place governing the use and maintenance of the system. These include SOPs covering change control, security, backup and restore, disaster recovery, contingency plans, and problem reporting and resolution. The SOPs will ensure the GCP-compliance is met during entire life cycle of the system.

3.10 Training and Implementation Strategy

3.10.1 Introduction to Training

Users will be trained on the system according to the SOP/controlled document “Training” prior to being granted system access. Functional training of users will occur using a database (Test database) separate from the productive database. Support personnel at the data centre will be trained on the operations and maintenance of the system prior to production implementation. Add any other training information related to the system implementation. To promote the system to production, all code and software modules will be migrated to the appropriate directories on the production servers.

3.10.2 Training

Training is a necessary component of achieving and using a validated state. Notice: the computerized system encloses users, training and documents associated with the proper use of the system. Training material has to be created. The importance of proper training cannot be underestimated. Training of personnel (specially of investigators) in clinical trials are essential to the proper conduct of clinical trials and finally for production of "safe, pure, and effective" drug products which are used in the maintenance of a healthy populace.

Each person engaged in data collection, monitoring, data management or study management shall have the necessary training, education, and experience, or any combination thereof, to enable that person to perform the assigned function. If should be one important aim of the data centre to provide this sort of training, to ensure quality in computer-supported clinical trials.

The validation of computer equipment is not valid unless the personnel operating the equipment during the testing have been properly trained. The personnel operating the equipment during this test period should be expected to operate this equipment once validation ends and normal production begins. It is the responsibility of each data centre’s head to ensure that their personnel are trained to perform the duties assigned to them (see table 5).

Table 5: Example for a list for Training Responsibilities

	Training Title	Trainer	Responsibilities	Time
1				
*2				

3				
4				
5				
…				

3.11 System Validation Maintenance and Support Strategy

3.11.1 Maintenance of the Validated State

To maintain the system in a validated state after release to the study production environment, controls will be in place. The system will be included within the scope of SOP "Backup and Restore", as well as the data centre's Disaster Recovery Plan. The system is part of the security infrastructure at the centre (see table 6). A contingency plan for system downtime or emergency situations should be developed. Any problems experienced with the system in its maintenance phase may be reported to a responsible party in accordance with SOP "Problem Reporting and Resolution". New users of the system will be trained prior to being granted access to use the production system. Any changes made to the system, including the technical architecture on which it resides, will be made in accordance with SOP Change Control.

Table 6: List of SOPs for Security Infrastructure and System Maintenance at the Data Centre

Nr.	SOP-Nr.	SOP-Titel	Responsibility
1			
2			
3			
4			
5			
…			

3.11.2 Support

The system will be supported by a responsible party at the data centre who will be responsible for:

- Maintaining the system history log
- Performing system monitoring
- Making recommendations to the Validation Team regarding system changes
- Creating, testing, and implementing changes in conjunction with the validation team
- Supporting users of the system in production, discuss any internal or external service level agreements (if applicable).

3.12 Requalification Criteria

Requalification of the system will take place for: certain measurable criteria which, when met, will initiate the requirement to qualify the system (list these criteria). This criteria may include "whole number" release of the software, greater than a certain number of problem reports or bugs addressed, greater than a certain percentage of the software modified, etc.).

3.13 Documentation Maintenance

Validation documentation will be archived in accordance with SOP Document Archival and Retrieval. Authorized personnel can retrieve these documents by contacting a responsible party. Data storage will be in accordance with SOP Backup and Restoration. The Responsible party will maintain an electronic copy of validation deliverables on site for reference.

3.14 Protocol Final Reports

3.14.1 Final Report

A final report will be written and approved upon the completion of execution of any qualification/validation protocol. This report will contain test data in raw and summary forms, and a conclusion of the acceptability of the qualification/ validation study and suitability of the system or process to meet qualification requirements.

3.14.2 Content

The final report will include the following sections as minimum requirements:

- An overview of the protocol execution activities
- Comparison of test and inspection results against acceptance criteria, based on the traceability matrix
- Documentation of any exceptional conditions or protocol deviations
- A risk assessment of the validation results.

Any exceptional conditions encountered during execution of a test protocol that could impact the process or study integrity, and reproducibility, will be identified, investigated and appropriate courses of action (justification, correction, requalification) determined. The Final report will be reviewed and approved by a functional department at the data centre and data centre's Quality Assurance. Final approval will constitute acceptance of the test data and the conclusion statement(s) and the formal acceptance of the system as having been qualified.

3.14.3 System Acceptance Criteria

Stable version of the system will be accepted under the following conditions:

- Structural testing results indicate that the system allows for successful execution of core study functions, that the system can recover from failure and restart successfully, that it can be successfully backed up and restored, and that its performance is acceptable even under stress conditions.
- Qualification testing results indicate that the system can be successfully installed in the target production environment of the data centre and that the target environment is in a stable, controlled state. Functional testing results indicate that all functional requirements defined as Critical and at least 90% of functional requirements ranked as "Important" test successfully. Additionally, adequate SOPs are in place and training completed to ensure continued operations and data integrity. Qualification

testing also indicates that clinical studies can be conducted with the software, without full control over patient data and with GCP-compliance.
- There are no system errors logged in the error log with a status of “Open” and a priority of “High”.

Results from all test phases will be summarized, conclusions derived and the Validation Team will provide approve/reject recommendations, based on the results and the predetermined acceptance criteria. The Validation Team and the System Owner will approve the Validation Final Report, and QA members of data centre will audit the report. Including in the final report are all other validation reports and documents as listed in validation deliverables (see table 7).

To consider a computer system to be validated the following steps should be performed and documentation in the SVMP provided:

- All Validation deliverables should be completed
- Developer evaluation/Vendor Audit performed and acceptance
- Life-cycle Concept
- Functional Description
- Functional Specification
- Hardware design - structural description
- Software Preparation - Under Quality Assurance Program
- Software Evaluation - off line, Simulation
- Installation Qualification
- Operational Qualification
- Performance Qualification
- Hardware Operation Qualification
- System Integration
- System security infrastructure
- Maintenance/Change control
- Security Measures

Table 7: Example list of Validation Reports

Document	**Project Validation Plan**	**Requirements Specifications**	**Functional Specification**	**Acceptance Testing**	**Installation Qualification**	**Operational Qualification**	**Performance Qualification**	**Security Plan**	**Change Control Continuity Plan**	**Protocol Final Reports**	**Validation Plan Final Report**
Project Manager											
System Owner											
Operations											
Data Centre Technician											
Technical Support											

Validation team											
Data Centre Quality Assurance											
Technical Writer											
Add and subtract as required											

Add and subtract as required

A: Approver	**R: Reviewer**	**C: Create Document**

4 Key Requirements according to CDISC and EU GCP Inspectors Working Group

In the following we enumerate the key requirements as set forward by the CDISC and the European Union's GCP Inspectors Workking Group.

4.1.1 Requirement #1

Requirement:	An instrument used to, capture, source data shall ensure that the data are captured as specified within the protocol.
Functionality:	The design of the eCRF forms and the system processing.

4.1.2 Requirement #2

Requirement:	An instrument used to, capture, source data shall ensure that the data are captured as specified within the protocol.

4.1.3 Requirement #3

Requirement:	Source data shall be Accurate, Legible, Contemporaneous, Original, Attributable, Complete and Consistent.
Functionality:	• The use of electronic capture should result in an improvement over a paper-based capture process. • Attributable needs to be assured by the system (login, username, password etc.). • Electronic entry eliminates problems with legibility • Use of identification mechanisms leads to attributable data • Completeness and consistency are advanced through the use of features such as drop-down lists of choices, online edits, check boxes, and branching based on entries. • Use of automatic system date/time stamps yields the ability to determine if entries were contemporaneous.

4.1.4 Requirement #4

Requirement:	An audit trail shall be maintained as part of the source documents for the original creation and subsequent modification of all source data.
Functionality:	The system needs to implement the audit trail requirement for the source data. This will be as part of the central database.

4.1.5 Requirement #5

Requirement:	The storage of source documents shall provide for their ready retrieval.
Functionality:	• The central server allows for ready retrieval. This requires assuring the server is available during times when all sites may need to access records • Records would need to be maintained on the central server for the regulatory retention period (and accessible by sites during this time) or archived and access provided to the sites.

4.1.6 Requirement #6

Requirement:	The investigator shall maintain the original source document or a certified copy.
Functionality:	Only a single copy is stored on the central server. Therefore this arrangement cannot meet the requirements.

4.1.7 Requirement #7

Requirement:	Source data shall only be modified with the knowledge or approval of the investigator.
Functionality:	• Within this arrangement, fraudulent or accidental amendment is possible since the investigator does not have a copy of the source data/documents. • Changes can be made without the approval of the investigator, but by having an audit trail immediately and readily available with the record, the investigator could become aware of changes, if periodic review is completed. However, administrative rights for a system may allow the audit trail to be circumvented.

4.1.8 Requirement #8

Requirement:	Source documents and data shall be protected from destruction.
Functionality:	• Steps can be taken at the central database to prevent destruction. However, fraudulent or accidental destruction is possible, due to the storage at a single location that is not the site. • The audit trail may provide evidence of record deletion but administrative rights for a system may allow the audit trail to be circumvented.

4.1.9 Requirement #9

Requirement:	The source document shall allow for accurate copies to be made.
Functionality:	• Copies can be made from the central database. • There is a need to define what is an accurate copy in an electronic sense.

	• Accurate copies must include the meaning of the data (for example, date formats), as well as the full audit trail. • The site would need to have the capability to review and generate copies.

4.1.10 Requirement #10

Requirement:	Source documents shall be protected against unauthorized access.
Functionality:	Sponsor can take steps to ensure that the contents of the central database are protected against unauthorized access. However, this should be under the Investigator's control.

4.1.11 Requirement #11

Requirement:	The sponsor shall not have exclusive control of a source document.
Functionality:	With this arrangement, the sponsor has exclusive control of the source data/documents.

4.1.12 Requirement #12

Requirement:	The location of source documents and the associated source data shall be clearly identified at all points within the capture process.

4.1.13 Requirement #13

Requirement:	When source data are copied, the process used shall ensure that the copy is an exact copy preserving all of the data and metadata of the original.

5 Standard Requirements for GCP-compliant Data Management in Multinational Clinical Trials

The standard requirements presented on this section are according to the publication "Standard requirements for GCP compliant data management in multinational clinical trials" of the European Clinical Research Infrastructures Network (ECRIN) Working Group on Data Centres Version 1 from 27 May 2010.

In general the requirements were developed by expert consensus of the ECRIN Working group on Data Centres, using a structured and standardised process. The requirements are divided into two main parts: an IT part covering standards for the IT infrastructure and computer systems in general, and a Data Management (DM) part covering requirements for data management applications in clinical trials.

The standard developed includes 115 IT-requirements, split into 15 separate sections, 107 DM-requirements (in 12 sections) and 13 other requirements (2 sections).

Each individual requirement is characterized by an original ID number and categorized as either a minimal (min) requirement or best practice (bp).

5.1 IT Requirements

All IT-requirements are split into 15 separate sections according to the standard requirements of the European Clinical Research Infrastructures Network (ECRIN) Working Group on Data Centres:

- IT01 - Procurement and Installation (Servers)
- IT02 - Physical Security and Management
- IT03 - Logical Security and Management
- IT04 - Logical Access Control
- IT05 - Business Continuity
- IT06 - General System Validation
- IT07 - Local Software Development
- IT08 - Clinical DBMS Systems
- IT09 - Treatment Allocation Systems
- IT10 – Reporting
- IT11 - Data Export
- IT12 - Importing & Uploading Data
- IT13 - Directly Amending Data
- IT14 - Delivery of Data for Analysis
- IT15 - Long Term (electronic) Data Curation

5.1.1 IT01 - Procurement and Installation (Servers)

5.1.1.1 IT01.01 min - Server Specification

Requirement:	Servers and similar equipment should be specified and selected according to the specific requirements of the trials unit and the functions being supported

5.1.1.2 IT01.02 min - Server Builds

Requirement:	Servers and similar equipment should be specified and selected according to the specific requirements of the trials unit and the functions being supported

5.1.1.3 IT01.03 min - Warranties and Support

Requirement:	Servers and similar equipment should be specified and selected according to the specific requirements of the trials unit and the functions being supported

5.1.1.4 IT01.04 bp - Server Procurement

Requirement:	Servers and similar equipment should be specified and selected according to the specific requirements of the trials unit and the functions being supported

5.1.1.5 IT01.05 bp - Procurement Planning

Requirement:	There should be a defined retirement/replacement policy for servers, given expected lifetimes

5.1.2 IT02 - Physical Security and Management

5.1.2.1 IT02.01 min - Locked Server Room

Requirement:	Servers must be housed within a dedicated locked room with unescorted access limited to specified individuals

5.1.2.2 IT02.02 min - Secured Power Supply

Requirement:	The power supply to servers should be secured, e.g. by a UPS unit, to allow an orderly shutdown on power failure

5.1.2.3 IT02.03 min - Encryption of non physically secure data

Requirement:	No patient data should be stored on anything other than protected servers (e.g. on laptops, desktops, USB sticks etc.) unless it is encrypted

5.1.2.4 IT02.04 min - Server Failure - Response

Requirement:	Alerts on server failure within normal business hours should be sent automatically to relevant personnel

5.1.2.5 IT02.05 bp - Server Failure - Response 24/7

Requirement:	Alerts on server failure outside of normal business hours should be sent automatically to relevant personnel

5.1.2.6 IT02.06 bp - Controlled Environment

Requirement:	Servers should be housed in a temperature-controlled environment

5.1.2.7 IT02.07 bp - Theft and Malicious Damage

Requirement:	The server room/building should have an alarm system with the alarm linked to a central response centre.

5.1.2.8 IT02.08 bp - Hazard Control - Fire Alarms

Requirement:	The server room should be fitted with heat and smoke alarms, monitored 24/7.

5.1.2.9 IT02.09 bp - Hazard Control - Fire Response

Requirement:	The server room should be fitted with automatic fire response measures (e.g. inert gas).

5.1.2.10 IT02.10 bp - Hazard Control - Water

Requirement:	Water ingress (e.g. from external flooding).

5.1.3 IT03 - Logical Security and Management

5.1.3.1 IT03.01 min - Security Management System

Requirement:	Regular reviews of IT security systems, practices and documentation, followed by any necessary planning and actions, should occur as part of an on-going Security Management System.

5.1.3.2 IT03.02 min - Commitment to Data Protection

Requirement:	The unit or its parent organisation can demonstrate compliance with and commitment to local data protection legislation, including relevant policies, training and individuals with designated roles (e.g. ‘Data protection officer’).

5.1.3.3 IT03.03 min - External Firewalls

Requirement:	External firewalls should be in place and configured to block inappropriate access.

5.1.3.4 IT03.04 min - Encrypted Transmission

Requirement:	Clinical data transmitted over the internet to or from the trials unit must be encrypted.

5.1.3.5 IT03.05 min Server Admin Role

Requirement:	Servers should be protected by a highly restricted administrator password (i.e. known to essential systems staff only).

5.1.3.6 IT03.06 min - Admin Password Management

Requirement:	The administrator password should be changed regularly according to locally agreed policies, and stored securely for emergency use (e.g. off site).

5.1.3.7 IT03.07 min - Server Maintenance

Requirement:	Necessary patches and updates should be identified and applied in a timely but safe manner to: • the operating system, • anti-malware systems, • backup systems and • major applications (e.g. Clinical DBMSs, Web servers, Remote Access systems, etc.)

5.1.3.8 IT03.08 bp - Commitment to Information Security

Requirement:	The unit or its parent organisation can demonstrate management commitment to information security, including relevant groups, policies, training and individuals with designated roles (e.g. 'IT security officer').

5.1.3.9 IT03.09 bp - Internal Firewalls

Requirement:	Internal firewalls should be in place and correctly configured, e.g. blocking access to other departments, students.

5.1.3.10 IT03.10 bp - Security Testing

Requirement:	Regular security testing should be carried out and is documented.

5.1.3.11 IT03.11 bp - Traffic Monitoring

Requirement:	Traffic activity should be monitored and hacking attempts identified and investigated.

5.1.4 IT04 - Logical Access Control

5.1.4.1 IT04.01 min - Logical Access Procedures

Requirement:	Standard Operating Procedures (SOPs) and policies for access control to the network(s) and specific systems should be in place.

5.1.4.2 IT04.02 min - Access Control Management

Requirement:	Each system requiring access controls should have mechanisms, e.g. using roles, group membership, etc., that can be used to effectively differentiate and manage access.

5.1.4.3 IT04.03 min - Granularity of Access

Requirement:	Access control mechanisms should be granular enough so that users only see the data they need to see.

5.1.4.4 IT04.04 min - Password management

Requirement:	Network password management should be enforced on all users, including regular password change and password complexity.

5.1.4.5 IT04.05 min - Remote Access

Requirement:	Remote access (e.g. via Citrix or certificate-based remote login) should be controlled to the same standards as above, and should not normally include access to the host's network.

5.1.4.6 IT04.06 min - Desktop Lockout

Requirement:	Desktop logins should post a blank screen or screensaver after a locally determined shut down period, and require password re-activation

5.1.4.7 IT04.07 min - Control - Clinical Data

Requirement:	Access rights to Clinical Data Systems should be regularly reviewed, changes to access requested and actioned according to defined procedures, by designated individuals, with records kept of all rights, when granted, why and by whom.

5.1.4.8 IT04.08 bp - Control - General

Requirement:	Access rights to the network and general should be regularly reviewed, changes to access requested and actioned according to defined procedures, by designated individuals, with records kept of all rights, when granted, why and by whom.

5.1.5 IT05 - Business Continuity

5.1.5.1 IT05.01 min - Business Continuity Plan

Requirement:	A Business Continuity plan should be present, covering likely action in the event of a major loss of function (e.g. fire, long term power failure, full server failure, sudden loss of key staff).

5.1.5.2 IT05.02 min - Back Up Policies

Requirement:	Documents detailing backup policy, procedures, restores and testing must be in place.

5.1.5.3 IT05.03 min - Back Up Frequency

Requirement:	Back ups must be taken at least once every 24 hours, using a managed, documented regime.

5.1.5.4 IT05.04 min - Back Up Storage

Requirement:	Back up media should be stored in a fire proof safe.

5.1.5.5 IT05.05 min - Recovery Testing

Requirement:	Testing of full restore procedures, back to the original server, should take place at least annually.

5.1.5.6 IT05.06 min - Off site archiving

Requirement:	The back up regime should involve regular offsite storage of archive media (e.g. monthly).

5.1.5.7 IT05.07 bp - Business Continuity Integration

Requirement:	The unit's Business Continuity (BC) should be integrated with the host organisation's BC plan and appropriate access arranged.

5.1.5.8 IT05.08 bp - Specified Downtime

Requirement:	A trials unit should state, and adhere to, a specific maximum downtime to any potential user.

5.1.5.9 IT05.09 bp - Business Continuity Review

Requirement:	Regular review, should occur, at least annually, of the detailed BC plan.

5.1.5.10 IT05.10 bp - Back up - Transaction Logs

Requirement:	Transaction log backups should take place regularly through the working day, according to a locally agreed plan.

5.1.5.11 IT05.11 bp - Back up - Environment

Requirement:	The server/DBA environment (groups, log-ins, jobs etc.) should be captured and restorable.

5.1.5.12 IT05.12 bp - Back up - Warm/Hot Failover

Requirement:	Log shipping or a mirroring procedure should be in place to a warm/hot failover system.

5.1.5.13 IT05.13 bp - Failover testing Recovery

Requirement:	If available, testing of full restore procedures from a warm/hot failover system should take place at least annually.

5.1.6 IT06 - General System Validation

5.1.6.1 IT06.01 min - Validation Policies

Requirement:	Policies and SOPs should be in place covering system validation systems and processes.

5.1.6.2 IT06.02 min - Validation master plan

Requirement:	The unit should have a validation master plan in place, identifying systems, the risks associated with each, and the consequent validation strategy for each.

5.1.6.3 IT06.03 min - Risk based approach

Requirement:	The general approach to validation of any system should be based on analysis of potential risk, and take into account the system's usage, users and origins.

5.1.6.4 IT06.04 min - Individual validation plans

Requirement:	Detailed validation plans should exist for any particular system, in line with the master plan and policies described above, detailing the validation required, how and when it should be done, and how it should be recorded.

5.1.6.5 IT06.05 min - Summaries and Recording

Requirement:	A signed and dated summary of the results of each major validation episode should exist, for each system being validated.

5.1.6.6 IT06.06 min - Detailed Evidence

Requirement:	More detailed evidence - e.g. of test results or signed user statements - should be available as evidence for the summary validation documents.

5.1.6.7 IT06.07 min - Change Control Policies

Requirement:	Policies and SOPs should be in place defining change control mechanisms and their scope, who should authorise and review requests, and how they should be documented.

5.1.6.8 IT06.08 min - Change and Re-validation

Requirement:	Changes in systems should result in a review of the need for revalidation.

5.1.6.9 IT06.09 min - Software Development

Requirement:	Evidence should be available that Quality Assurance (QA) processes during software development have been implemented properly.

5.1.7 IT07 - Local Software Development

5.1.7.1 IT07.01 min Documentation of in-house software

Requirement:	All modules should be fully documented and specify inputs, outputs, purpose as well as a description of internal mechanisms and algorithms.

5.1.7.2 IT07.02 bp - Code Review

Requirement:	Regular review and walk through of program code should occur.

5.1.7.3 IT07.03 bp - Re-usable Modules

Requirement:	A library of reusable validated code/modules/components should be developed.

5.1.7.4 IT07.04 bp - Development Model

Requirement:	A V-model based procedure is recommended, with constituent modules first validated individually and then integrated before re-validation at the system level.

5.1.7.5 IT07.05 bp - In line Commenting

Requirement:	All code should have sufficient in line documentation to support tracing of program execution.

5.1.8 IT08 - Clinical DBMS Systems

5.1.8.1 IT08.01 min - Development and Production Instances

Requirement:	The system offers two instances: development and production.

5.1.8.2 IT08.02 min - Timestamp Control

Requirement:	Time synchronization within the Clinical Data Management System (CDMS) is ensured. Sites using electronic Remote Data Capture (eRDC) are not able

	to change the system's time stamp.

5.1.8.3 IT08.03 bp - Metadata Audit Trail

Requirement:	An audit trail for metadata changes is implemented.

5.1.8.4 IT08.04 bp - Available audit trail

Requirement:	The audit trail for any particular data item is visible.

5.1.8.5 IT08.05 bp - Searchable audit trail

Requirement:	The audit trail is searchable and capable of producing audit trail reports.

5.1.8.6 IT08.06 bp - Development, Production and Test Instances

Requirement:	The system offers three instances: development, test, production. The test environment and the production environment are identical.

5.1.8.7 IT08.07 bp - Latin Characters

Requirement:	Systems support a full range of accented Latin characters.

5.1.8.8 IT08.08 bp - Date/numerical Representation

Requirement:	It is possible to set and use different date and numerical representations in the system.

5.1.9 IT09 - Treatment Allocation Systems

5.1.9.1 IT09.01 min - Documentation & Validation

Requirement:	The underlying logic and operations of all systems for allocating subjects to treatments must be clearly documented and validated.

5.1.9.2 IT09.02 min - Record of Allocation

Requirement:	A record of all allocation material generated (e.g. randomisation lists) and all decisions made (e.g. within a dynamic balancing system) must be maintained.

5.1.9.3 IT09.03 min - Failover to Manual

Requirement:	System(s) must be in place, supported by training, to deal with a loss of normal electronic randomisation.

5.1.9.4 IT09.04 bp - Monitoring

Requirement:	The randomness of list generation or minimisation should be monitored in the context of any particular trial.

5.1.10 IT10 - Reporting

5.1.10.1 IT10.01 min - Report access control

Requirement:	Access to different reports should be controlled and match the users' requirements.

5.1.10.2 IT10.02 min - Report Validation

Requirement:	The structure and accuracy of reports should be validated against the source data, frequency of validation being determined by a change control process.

5.1.10.3 IT10.03 min - Single Subject Data

Requirement:	It should be possible to examine and export a full record of a single subject's data (excluding personal identifying data).

5.1.10.4 IT10.04 bp - Standard Reports

Requirement:	A set of frequently required (parameterised) reports should be available to appropriate users.

5.1.10.5 IT10.05 bp - UI Ad Hoc Reports

Requirement:	It should be possible to extract ad-hoc filtered datasets (reports) via the UI.

5.1.10.6 IT10.06 bp - Audit Data

Requirement:	Selected reports should include the option of including audit related data.

5.1.10.7 IT10.07 bp - Report Rerun

Requirement:	Once a report is parameterised by user it should be possible to save and

	rerun it.

5.1.10.8 IT10.08 bp - Metadata included

Requirement:	The option should exist to include a metadata description of extracted data.

5.1.10.9 IT10.09 bp - Study definition

Requirement:	Standard reports should include the details of the current study definition in an approved XML schema (trial schedule and data items).

5.1.10.10 IT10.10 bp - Format of Reports

Requirement:	Report data can be generated/exported in formats agreed with local report consumers , e.g. PDF, HTML, XML.

5.1.10.11 IT10.11 bp - Data Personnel

Requirement:	It should be possible to examine and export a record of a single data entry clerk's input data.

5.1.10.12 IT10.12 bp - Key Field Changes

Requirement:	It should be possible to examine and export a full list of changes to identified key fields, e.g. fields reporting toxicity as part of monitoring.

5.1.10.13 IT10.13 bp - Automatic Generation

Requirement:	The generation of reports can be automated and can be scheduled.

5.1.11 IT11 - Data Export

5.1.11.1 IT11.01 min - Data Export Procedures

Requirement:	SOPs and policies for data exports should be in place.

5.1.11.2 IT11.02 min - Encryption of PID

Requirement:	The inclusion of any patient identifiable data means any exported file(s) must be encrypted.

5.1.11.3 IT11.03 min - Purpose Recorded

Requirement:	The purpose of the planned data transfer(s) and the nature of any further processing/transfer planned for the data should be known and logged.

5.1.11.4 IT11.04 min - Assuring Security

Requirement:	The unit sending the data must have a written agreement/declaration from the recipient that the receiving organization will maintain appropriate security of data.

5.1.11.5 IT11.05 min - Records of Transfers

Requirement:	Details of any specific data transfer should be logged, including list of data items, sender, recipient and transfer method, and the date sent.

5.1.11.6 IT11.06 min - Retention of Copies

Requirement:	Copies of the data sent should be retained within a read only regime and be available as a reference data set for audit/reconstruction purposes.

5.1.11.7 IT11.07 bp - Format of Transfers

Requirement:	The format of data should be as specified by the recipient.

5.1.11.8 IT11.08 bp - Electronic Archiving

Requirement:	Standardised formats for electronic archiving (e.g. ASCII, PDF, XML, CDISC ODM, FDA approved SAS format) are used.

5.1.12 IT12 - Importing & Uploading Data

5.1.12.1 IT12.01 min - Upload Procedures

Requirement:	SOPs and policies for importing/uploading data should be in place.

5.1.12.2 IT12.02 min - File Retention I

Requirement:	The original files received should be retained within a read only regime, and be available as a reference data set for audit/reconstruction purposes.

5.1.12.3 IT12.03 min - Logging of Uploads

Requirement:	Each upload process should be documented and logged.

5.1.12.4 IT12.04 bp - File Retention II

Requirement:	Any files prepared from the originals and used as the direct source of the upload should be kept securely within a read only regime for audit/reconstruction purposes.

5.1.12.5 IT12.05 bp - Data Validation on Input

Requirement:	Data uploaded to clinical data systems should be checked and annotated as per normal data entry.

5.1.13 IT13 - Directly Amending Data

5.1.13.1 IT13.01 min - Requests for Amendment

Requirement:	Any requests must be in writing and retained, and must include the justification for the change.

5.1.13.2 IT13.02 min - Recording Amendments

Requirement:	Any changes made must be logged and the details noted.

5.1.14 IT14 - Delivery of Data for Analysis

5.1.14.1 IT14.01 min - Preparation for Analysis Procedures

Requirement:	SOPs and policies for generating and preserving datasets for analysis should be in place.

5.1.14.2 IT14.02 min - R/O Analysis Data Retention

Requirement:	The base data provided for analysis is retained within a read only regime, and is available is a reference data set for any future re-analysis or audit.

5.1.14.3 IT14.03 min - Extracted Data Validation

Requirement:	The data generated for analysis, and/or the extraction process, should be validated against the source data in the clinical database (not necessarily by IT staff).

5.1.14.4 IT14.05 bp - Extracted Data - Formats

Requirement:	The data generated can be generated in Stata, SAS, R and SPSS native formats (as well as CSV, XML).

5.1.15 IT15 - Long Term (electronic) Data Curation

5.1.15.1 IT15.01 min - Data Preparation Policies

Requirement:	Policies/SOPs about what data would normally be curated (should normally include metadata, the protocol and other documents as well as all clinical data) should be in place.

5.1.15.2 IT15.02 min - Data Retrieval from Curation

Requirement:	Policies/SOPs about how data would normally be retrieved/ accessed, and who is authorised to do so by the sponsor/investigator, should be in place.

5.1.15.3 IT15.03 min - Data Destruction

Requirement:	Final destruction of data, if required /allowed, should be as specified by regulations, funding body and/or sponsor.

5.1.15.4 IT15.04 min - Recovery Testing

Requirement:	The recovery process(es) should be documented and tested.

5.1.15.5 IT15.05 bp - Data Preparation formats

Requirement:	Data from databases should be decrypted if necessary and transformed into pre-approved XML schemas (e.g. CDISC ODM, Data Documentation Initiative (DDI) 3), or into plain ASCII text files.

5.1.15.6 IT15.06 bp - Data Preparation - Identifiers

Requirement:	Subject identifiers should be reduced to a minimum or removed altogether, depending on policies/requirements.

5.1.15.7 IT15.07 bp - Data Preparation - Records

Requirement:	The data preparation process, its inputs, dates and details, should be logged.

5.1.15.8 IT15.08 bp - Additional Material Generation

Requirement:	Additional electronically stored material may be generated to ensure copies of paper only documents are available (i.e. by scanning).

5.1.15.9 IT15.09 bp - Curation Facilities

Requirement:	Service level agreements should be in place with specialist curation providers, providing physical and logically secure long term storage.

5.2 Data Management Requirements

5.2.1 DM01 - Clinical Data Management Application - Design and Development

5.2.1.1 DM01.01 min - Development Lifecycle Policy

Requirement:	SOPs covering the development lifecycle of the clinical data management application and the CRF (incl. development, testing and deployment) should be in place.

5.2.1.2 DM01.02 min - Design of CRFs

Requirement:	Process of CRF design is documented, reviewed and includes version management.

5.2.1.3 DM01.03 min - Cross-disciplinary Team

Requirement:	Clinical data management application and CRF development is performed by a cross- disciplinary team (e.g. programmer, trial manager, statistician, data manager).

5.2.1.4 DM01.04 min - Requirement Specifications of CRF

Requirement:	The requirements specification for the CRF is driven by the protocol (e.g. primary safety and efficacy variables) and takes into consideration the workflow of trial procedures and organizational aspects.

5.2.1.5 DM01.05 min - Standardized Questionnaires/Instruments

Requirement:	Validated questions, scales or standard instruments are used where possible (e.g. quality of life questionnaires) and the integrity of validated questionnaires is maintained.

5.2.1.6 DM01.06 min - Data Non-redundancy

Requirement:	CRF does not duplicate data (e.g. no redundant questions, if not for validation/data management purposes) or calculates results unnecessarily.

5.2.1.7 DM01.07 min - Functional Specifications of CRFs

Requirement:	CRF functional specifications exist identifying each data item on each CRF (including field names, types, units, validation logic, conditional branching).

5.2.1.8 DM01.08 min - Checking of clinical data management application

Requirement:	Procedures are implemented for checking (e.g. proofreading) the clinical data management application including eCRF and pCRFs against specifications and protocol.

5.2.1.9 DM01.09 min - Delivery of CRFs

Requirement:	CRFs are delivered to sites prior to enrolment.

5.2.1.10 DM01.10 min - Evaluation of CRF Usability

Requirement:	The usability of eCRFs is evaluated and assessed before deployment to live environment.

5.2.1.11 DM01.11 bp - Review of CRFs

Requirement:	CRFs are reviewed against the protocol, end-user expectations and CRF design best practice (e.g. use of validated questionnaires). An acceptance test for CRFs is conducted.

5.2.1.12 DM01.12 bp - Use of Interim CRF

Requirement:	In cases of eCRF an interim CRF (iCRF) should be available to allow data to be accurately recorded/collated at sites prior to data entry for emergency cases (e.g. if eCRF not available).

5.2.1.13 DM01.13 bp - Documentation Principles

Requirement:	Common documentation principles are applied to data items (e.g. preferred coding system, numbering of items, types of missing data, complete answer categories, preference for positive formulated questions, etc.).

5.2.1.14 DM01.14 bp Libraries and Metadata Repositories

Requirement:	Libraries with procedures concerning library management and/or a metadata repository are used, enabling reuse of predefined data items/forms.

5.2.1.15 DM01.15 bp - Quality Management

Requirement:	Quality documents covering good design practice, usability, local design conventions, etc. are available.

5.2.1.16 DM01.16 bp - User Friendliness of CRFs

Requirement:	CRFs are divided into appropriate sections with simple and clear instructions for completion and use consistent design principles.

5.2.2 DM02 - Clinical Data Management Application – Validation

5.2.2.1 DM02.01 min - Clinical Data Management Application Policies

Requirement:	SOPs and policies for clinical data management application and CDMS validation are in place.

5.2.2.2 DM02.02 min - Trial-specific Test Plan

Requirement:	A trial-specific test plan defines the test methodology, covering scope of test, item pass/fail criteria, etc..

5.2.2.3 DM02.03 min - Test against Functional Specifications

Requirement:	The testing with sample data against functional specifications is carried out before deployment to live environment.

5.2.2.4 DM02.04 min - Test of Data Checks

Requirement:	Tests of all validation checks and conditional data capture mechanisms, plus any derivations are conducted, documented and retained.

5.2.2.5 DM02.05 min - Validation Report

Requirement:	Data validation final report for the trial has to be provided and signed by responsible DM person.

5.2.2.6 DM02.06 min - CRF Approval

Requirement:	Approval of the CRF is signed off by key persons.

5.2.2.7 DM02.07 min - Check of Validation Programs, Lists and Scripts

Requirement:	Validation programs, lists and scripts are checked, tested, documented and retained.

5.2.2.8 DM02.08 bp - Validation against Specifications

Requirement:	The process of clinical data management application design and data checks programming is validated against specifications.

5.2.2.9 DM02.09 bp - Validation Report Generation

Requirement:	System is able to generate reports used for validation.

5.2.3 DM03 - Clinical Data Management Application - Change management

5.2.3.1 DM03.01 min - Change Management of Clinical Data Management Application

Requirement:	SOPs and policies for clinical data management application change management are in place, including last minute chances.

5.2.3.2 DM03.02 min - Change Management of Metadata

Requirement:	Individual requests for change to metadata (e.g. meta-data, specification of CRF) are justified, itemized and recorded by authorised personnel.

5.2.3.3 DM03.03 min - Amendment for Change

Requirement:	A risk analysis is conducted before major amendment for change. For each major change the changes, implications and consequent further actions are recorded.

5.2.3.4 DM03.04 min - Test of Amendments

Requirement:	Any amendment is tested in the test environment, following test specifications and the test results are recorded.

5.2.3.5 DM03.05 min - Renewed Training

Requirement:	In the case of significant changes, the need for retraining is evaluated and implemented if necessary.

5.2.3.6 DM03.06 min - Information of Changes

Requirement:	Mechanisms are implemented to easily inform relevant staff and users of changes, and provide support and explanatory material as required.

5.2.3.7 DM03.07 bp - Requirements for amended CRF

Requirement:	An amended CRF (that may require ethical approval) has to conform to requested amendments and/or revised protocol. Trial amendments, that may have consequences on the CRF, are taken into consideration.

5.2.3.8 DM03.08 bp - CRF-versioning

Requirement:	CRF page numbering and version information is always updated to reflect the current status.

5.2.3.9 DM03.09 bp - Management of Change Requests

Requirement:	Change requests are accumulated to minimize amendments.

5.2.4 DM04 - Treatment Allocation and (Un)Blinding Management

5.2.4.1 DM04.01 min - Policies for the Implementation of Randomisation

Requirement:	SOPs and policies for the set up of randomisation in any particular trial are in place.

5.2.4.2 DM04.02 min - Policies for ensuring Randomisation/Blinding

Requirement:	SOPs and policies exist for protection of blinding and conservation of random allocation to treatment groups.

5.2.4.3 DM04.03 min - Policies for Unblinding

Requirement:	SOPs are in place to support rapid and safe unblinding of blinded treatments.

5.2.4.4 DM04.04 min - Specification of Randomisation

Requirement:	Specification for the underlying system(s) or the specific trial randomisation process is available.

5.2.4.5 DM04.05 min - Randomisation Implementation

Requirement:	The randomisation implementation for any particular trial conforms to the protocol.

5.2.4.6 DM04.06 min - Specification of the Randomisation Design

Requirement:	The study statistician is responsible for the specification of the randomisation design. A randomisation specification document is provided.

5.2.4.7 DM04.07 min - Problem Management of Randomisation

Requirement:	Any problems that arise in the randomisation process are logged and the subsequent actions recorded.

5.2.4.8 DM04.08 min - Randomisation Training

Requirement:	All staff who handles randomisation requests is adequately trained for each specific trial randomisation process.

5.2.5 DM05 - Site Management, Training and Support

5.2.5.1 DM05.01 min - Policies for Site Opening

Requirement:	SOPs or policies for opening a centre for data collection are in place.

5.2.5.2 DM05.02 min - User Training for Data Entry

Requirement:	User training with data entry instructions or guidelines, for both pCRFs and eCRFs, is provided for relevant site staff and is documented.

5.2.5.3 DM05.03 min - Test or Productive Environment

Requirement:	It is clearly indicated to the user whether they are working on a test eCRF or whether the “real trial” has been opened.

5.2.5.4 DM05.04 min - Access to Production System

Requirement:	Site has access to production data systems only once all relevant paperwork and training has been completed; including ethical and research approvals, contracts, site initiation.

5.2.5.5 DM05.05 min - Site Documentation

Requirement:	After significant changes site documentation is updated.

5.2.5.6 DM05.06 min - Responsibility list

Requirement:	An up to date list of who can do what at each site, including complete CRFs, i.e. a 'delegate log', is maintained.

5.2.6 DM06 - Data Entry and Processing

5.2.6.1 DM06.01 min - Data Entry Policies

Requirement:	SOPs and policies for data entry and corrections are in place.

5.2.6.2 DM06.02 min - Restriction of Data Access

Requirement:	Site staff have access only to data of their site.

5.2.6.3 DM06.03 min - Data Security

Requirement:	Data manager and IT-staff involved will keep data secure and confidential at all times.

5.2.6.4 DM06.04 min - System Security

Requirement:	System security and access control is ensured, data is only accessible to authorised personnel.

5.2.6.5 DM06.05 min - Tracking of CRFs

Requirement:	A CRF tracking system is in place.

5.2.6.6 DM06.06 min - Management of missing CRFs

Requirement:	Systems identify and report on missing or late CRFs /data.

5.2.6.7 DM06.07 min - Quality of Received Data

Requirement:	Data received is checked (pCRF and eCRF).

5.2.6.8 DM06.08 min - Data Confidentiality

Requirement:	The blinding of information submitted to the data centre with regard to subject identifying information conforms to national requirements (pseudonymisation).

5.2.6.9 DM06.09 min - Self Evident Corrections

Requirement:	Clear guidelines and procedures exist to carry out self evident corrections.

5.2.6.10 DM06.10 min - Simple Checks

Requirement:	Simple checks (e.g. range checks) should be available with the possibility to unset for pCRF entry.

5.2.6.11 DM06.11 min - Complex Checks

Requirement:	Complex checks with critical variables (e.g. crossform validation) are available.

5.2.6.12 DM06.12 min - Audit Trail

Requirement:	All transactions to the trial database (insert, update, delete) have a clear and complete audit trail, covering the date and time of the input, the person making the change and the old and new values.

5.2.6.13 DM06.13 bp - Timelines for Data Entry

Requirement:	Time-lines for data entry are considered.

5.2.6.14 DM06.14 bp - Amendment/Truncation of Schedules

Requirement:	Logging systems can easily truncate and/or amend schedules to maintain accuracy in identifying outstanding data.

5.2.6.15 DM06.15 bp - Data Deletion

Requirement:	Complete deletion of data from the system is prevented unless it is to comply with a legal request. If indicated for legal reasons, total deletion only takes place using specified procedures and recording with explanatory information.

5.2.7 DM07 - Data Quality Checks

5.2.7.1 DM07.01 min - Data Quality Policies

Requirement:	SOPs and policies are in place regarding data checking, and refer as necessary to the protocol, agreed instructions, GCP and regulatory requirements.

5.2.7.2 DM07.02 min - Batch Validation Checks

Requirement:	Validation checks are able to be executed via a batch process, to identify new warnings, missing, illogical and inconsistent data.

5.2.7.3 DM07.03 min - Data Review

Requirement:	Systems are able to support data checks by generating specified data in formats that match input format (e.g. that mimic CRFs) for manual review of data, e.g. medical consistency checks, lab data pointing to an AE.

5.2.7.4 DM07.04 min - Risk Based Source Data Verification

Requirement:	A risk based source data verification regime is implemented as specified in the protocol, with the emphasis on primary target variables and other essential data. A check of primary endpoints and other essential data is conducted.

5.2.7.5 DM07.05 min - Documentation of Checks

Requirement:	All data checking exercises are documented.

5.2.7.6 DM07.06 min - Problem Management

Requirement:	Problems and issues are reported to the appropriate person for query generation or other resolution.

5.2.7.7 DM07.07 bp - Quality Monitoring of Sites

Requirement:	Centres are monitored for quantity/types of errors to identify potential

	problems, e.g. with particular preset trigger levels.

5.2.7.8 DM07.08 bp - Statistical Evaluation of Data Quality

Requirement:	Statistical methods are used to assess and evaluate data quality (e.g. measures to analyse possible problems and irregularities should cover e.g. multivariate analysis of possible outlier candidates, conspicuous data patterns, preferred numerical sequences, accumulation of values close to defined limits) and the impact on analysis should be evaluated.

5.2.8 DM08 - Query Management

5.2.8.1 DM08.01 min - Query Policies

Requirement:	SOPs and policies are available covering query format, generation, timelines, data change and resolution.

5.2.8.2 DM08.02 min - Query Resolution

Requirement:	Procedure for resolving of queries exist.

5.2.8.3 DM08.03 min - Query Creation and Tracking

Requirement:	Queries are created in accordance with specifications and documented procedures.

5.2.8.4 DM08.04 min - Responses to Queries

Requirement:	Responses are recorded when returned, identified when outstanding and resent as necessary.

5.2.8.5 DM08.05 min - Actions in Response to Queries

Requirement:	Query resolution tracked and appropriate action taken within agreed timelines and documented in the audit trail.

5.2.8.6 DM08.06 bp - Issuing of Queries

Requirement:	Queries are issued to sites within agreed timelines.

5.2.8.7 DM08.07 bp - Avoidance of Query Duplications

Requirement:	Systems avoids accidental duplication of queries.

5.2.8.8 DM08.08 bp - Generation of Messages

Requirement:	System is able to generate messages to users not linked to specific data items (i.e. information giving, not expecting a reply).

5.2.8.9 DM08.09 bp - Generation of Query Reports

Requirement:	Reports are generated showing query generation data, return times etc. broken down by site, by source form, etc..

5.2.9 DM09 - Data Coding and Standards

5.2.9.1 DM09.01 min - Policies for Coding

Requirement:	SOPs and policies for coding are in place (e.g. to promote consistency and proper use of versions).

5.2.9.2 DM09.02 min - Coding Training

Requirement:	Coding or categorisation is carried out by personnel trained on the relevant systems.

5.2.9.3 DM09.03 min - Support of CONSORT

Requirement:	The protocol, clinical data management application and CRF, should support the CONSORT trial reporting requirements.

5.2.9.4 DM09.04 min - Coding of SAEs

Requirement:	The constituent symptoms of all Serious AEs are coded prior to analysis (e.g. MedDRA for drugs).

5.2.9.5 DM09.05 bp - Use of Standards for Coding

Requirement:	Coding uses named standard systems for particular types of data (e.g. MedDRA) where possible.

5.2.9.6 DM09.06 bp - Consistency of Coding

Requirement:	Coding uses consistent systems across different trials and follow consistent conventions and rules in their use.

5.2.9.7 DM09.07 bp - Coding of AEs

Requirement:	The constituent symptoms of all AEs should be coded prior to analysis.

5.2.9.8 DM09.08 bp - Autocoding

Requirement:	Use of autoencoder(s) and synonym list(s) where possible, however within well defined limits and with authorisation from senior staff, otherwise manual coding is performed.

5.2.10 DM10 - Safety Data Management Application

5.2.10.1 DM10.01 min - Policies for Safety Data Management

Requirement:	SOPs and policies for safety data management are in place.

5.2.10.2 DM10.02 min - Safety Data Management

Requirement:	Safety data management application allow the logging of all forms, faxes and correspondence involved, and subsequent information/evaluation requests.

5.2.10.3 DM10.03 min - Expedited Reporting

Requirement:	Safety data management application supports expedited reporting to authorities.

5.2.10.4 DM10.04 min - Routine Reporting

Requirement:	Safety data management application supports routine reporting to all relevant authorities when required (e.g. annual line listings).

5.2.10.5 DM10.05 bp - Electronic Reporting

Requirement:	Safety data management application supports reporting via electronic transfer to authorities.

5.2.10.6 DM108.06 bp - Safety Data Reconciliation

Requirement:	Safety data management application supports the reconciliation of SAEs with other safety data.

5.2.11 DM11 - Pre-Analysis Data Management

5.2.11.1 DM11.01 min - Policies for Data Base Locking

Requirement:	SOPs and policies regarding taking a fixed image of the database (snapshot) and, if required, 'locking' and 'unlocking' databases are in place. In case a locked database is unlocked a documented reason is provided.

5.2.11.2 DM11.02 min - Data Completion

Requirement:	All relevant data (or all except for a pre-defined/preagreed fraction) have been received prior to data extraction for analysis (database lock).

5.2.11.3 DM11.03 min - Query resolution completion

Requirement:	All queries (or all except for a pre-defined/pre-agreed fraction) have been resolved.

5.2.11.4 DM11.04 min - Data Reconciliation

Requirement:	All external data (e.g. safety database, lab data) has been reconciled.

5.2.11.5 DM11.05 min - Data Base Consistency Check

Requirement:	Relevant batch consistency checks of database have been completed and actioned.

5.2.11.6 DM11.06 bp - Review of Coding

Requirement:	All relevant coding has been reviewed.

5.2.11.7 DM11.07 bp - Data Base Audit

Requirement:	Database audit should be carried out, documenting error rate.

5.2.12 DM12 - Managing (physical) Archives

5.2.12.1 DM12.01 min - Policies for Archiving

Requirement:	SOPs and policies are in place concerning physical archiving of essential trial documents.

5.2.12.2 DM12.02 min - Access to Archive

Requirement:	Access to study archive is documented.

5.2.12.3 DM12.03 min - Protection of Archive

Requirement:	Measures are in place to guarantee safe archiving (e.g. locked rooms and fire-proof cupboards, safe area, protected and controlled access for authorized staff only).

5.2.12.4 DM12.04 min - Archiving Duration

Requirement:	Essential trial documents (including data) are archived for as long as specified by protocol, regulations, funding body and/or sponsor.

5.2.12.5 DM12.05 min - Trial Reconstitution

Requirement:	Conduct of trial can be reconstituted from archived essential trial documents.

5.3 International Aspects Requirements

5.3.1 IN01 - International Aspects

5.3.1.1 IN01.01 min - User Support

Requirement:	eRDC Help Desk and Hot Line is provided covering user hours.

5.3.1.2 IN01.02 bp - CRF Translation

Requirement:	If necessary, CRFs/eCRFs can be translated into the language(s) required for the trial, including messages associated with error checking. Translations are verified.

5.3.1.3 IN01.03 bp - Support of National Regulations

Requirement:	Application display, change or hide questions/CRFs to better support national legislation (without using different versions).

5.3.1.4 IN01.04 bp - Multilingual User Support

Requirement:	Help desk and hot line can deal with the language of the users and provide some sort of help.

5.4 Trials Unit Staff Competence Requirements

5.4.1 SC01 - Trials Unit Staff Competence

5.4.1.1 SC01.01 min - Policies for Training

Requirement:	SOPs and policies are in place describing induction and training requirements/policies/procedures.

5.4.1.2 SC01.02 min - Staff Competence

Requirement:	DM-staff is competent, trained or being trained to do the job(s) required of them.

5.4.1.3 SC01.03 min - Documentation of Training

Requirement:	Records of training are kept for all DM-staff, kept centrally and/or by the staff themselves.

5.4.1.4 SC01.04 min - Staff Support

Requirement:	Help and support for DM-staff is available.

5.4.1.5 SC01.05 bp - Planning of Staff Training

Requirement:	Training plans are linked to annual appraisal.

5.4.1.6 SC01.06 bp - Ticketing System

Requirement:	A formal mechanism for requesting support and logging requests/actions should exist.

.

6 Requirements of FDA Title 21 CFR Part 11[3]

For the FDA human subject protection is the most important aspect of GCP; therefore FDA has unique GCP responsibilities relating to decision-making on applications. The FDA system for human subject protection consists of:

- IRBs/Institutions
- Real-time oversight of safety data
- Effective sponsor monitoring
- Clinical investigators and site staff
- Responsiveness to subject concerns/complaints

FDA's aim is to strengthen the IRB System using the process of IRB registration to build an IRB inventory. For this purpose, FDA is working closely with OHRP, HSRS, and IOM toward piloting voluntary IRB accreditation. Ethics committee inspections play an important part for FDA[4]. The aimed for real-time oversight of safety covers the clinical investigator and site staff, education and the appropriate use of Data Monitoring Committees (DMC). FDA will issue guidance on DMC to assist sponsors in determining when a DMC is needed for optimal study monitoring. Protection of humans in clinical trials focuses particularly on the attention to vulnerable populations and the support by FDA paediatric initiatives[5] to obtain more data/labelling information. In addition, better protection for pregnant women, human foetuses, and neonates involved in research is an FDA aimed.

6.1.1 Standards for Non-US Trials

An increasing proportion of data submitted to NDA's is Non-US data. Criteria for accepting non-US, non-IND data has been vague and was often based only on the ethical principles of the Declaration of Helsinki. In this context, FDA has made progress in GCP harmonization and is moving toward GCP as a more concrete standard for accepting non-US, non-IND data. In addition, other harmonization efforts (WHO, PAHO, GHTF/ISO) have been expanded. For example, it is expected that research misconduct should be reported immediately. In such a case, sponsors should report: any information they have that any person involved in human subject trials committed research misconduct, whenever the sponsor discovers misconduct. For FDA education is the key to improving trial quality: GCP education must target all clinical trial participants and should be a process of "lifelong learning".

FDA established a new office to coordinate GCP across the agency and beyond: Office for Good Clinical Practice (OGCP). This office has following functions:

- GCP policy (bridging the centres and ORA)
- Bioresearch monitoring of clinical trials
- GCP initiatives
- International GCP (harmonization) activities
- GCP education and outreach
- FDA GCP/Human Subject Protection Steering Committee (medical policy)
- BIMO GCP round table
- Centre and ORA infrastructures

[3] Content for this section i staken from Deliverable D5.5

[4] David A. Lepay: Ethics Committee (IEC) Inspections. APEC GCP Inspection Workshop. May 30, 2008

[5] Interim Rule ("Subpart D"; Effective April 30, 2001): Additional Safeguards for Children in Clinical Investigations of FDA-Regulated Products

6.1.2 Critical Path Initiative

The Critical Path Initiative (CPI)[6] is an US strategy to drive innovation in science processes through which medical products are developed, evaluated, and manufactured. The initiative was launched in 2004, with the release of FDA's report "Innovation/Stagnation"[7] that diagnosed the reasons for the gap between successful scientific discoveries that have unlocked the potential to prevent and cure some of today's biggest diseases (diabetes, cancer, and Alzheimer's Disease) and the translation of basic discoveries into innovative medical treatments. Medical product development has become increasing difficult, expensive and unpredictable. The conclusion of the report was that actions to modernise scientific and technical tools, and to harness information technology to evaluate and predict the safety, effectiveness, and manufacturability of medical products are needed. Globalization, rapidly evolving technologies, and emerging areas of science all have an impact on FDA-regulated medical products.

6.1.3 Advancing Regulatory Science

Regulatory Science is the science of developing new tools, standards, and approaches to assess the safety, efficacy, quality, and performance of all FDA-regulated products. In 2010 FDA launched its Advancing Regulatory Science Initiative (ARS)[8], building on existing programs, like the Critical Path Initiative. ARS will cover every dimension of regulatory science. FDA and the National Institutes of Health (NIH) created an initiative to accelerate the process from scientific breakthrough to the availability of new, innovative medical therapies for patients[9]. The initiative involves two scientific disciplines: translational science (bringing basic scientific discoveries into treatments) and regulatory science (development and use of new tools, standards and approaches for more efficiency in the development of medicinal products and better evaluation of product safety, efficacy and quality). As part of this effort, FDA will establish a Joint NIH-FDA Leadership Council to lead collaborative work on important public health issues. It will help to ensure that regulatory considerations form an integral component of biomedical research planning. Following areas are addressed:

- Modernize Toxicology to Enhance Product Safety
- Stimulate Innovation in Clinical Evaluations and Personalized Medicine to Improve Product Development and Patient Outcomes
- Support New Approaches to Improve Product Manufacturing and Quality
- Ensure FDA Readiness to Evaluate Innovative Emerging Technologies
- Harness Diverse Data through Information Sciences to Improve Health Outcomes
- Implement a New Prevention-Focused Food Safety System to Protect Public Health
- Facilitate Development of Medical Countermeasures to Protect Against Threats to U.S. and Global Health and Security

6.1.4 GCP/Clinical Trial Notices

Notices related to Good Clinical Practice and the conduct of clinical trials are published by FDA:

- Clinical Trials Transformation Initiative

[6] http://www.fda.gov/ScienceResearch/SpecialTopics/CriticalPathInitiative/default.htm

[7] FDA: Challenges and Opportunities Report. Innovation or Stagnation: Challenge and Opportunity on the Critical Path to New Medical Products (March 2004)

[8] Advancing Regulatory Science at FDA: A Strategic Plan (August 2011)

[9] NIH News: NIH and FDA Announce Collaborative Initiative to Fast-track Innovations to the Public (24.2.2010). Online: http://www.nih.gov/news/health/feb2010/od-24.htm

- FDA/NCI MOU Regarding Common Standards-Based Data Repository
- Pilot program for the submission of electronic case report forms in XML format
- FDA Announces New Initiative to Modernize the Regulation of Clinical Trials and Bioresearch Monitoring
- Running Clinical Trials
- Guidance Documents and Notices
    - Information Sheet Guidance for Institutional Review Boards (IRBs), Clinical Investigators, and Sponsors
    - Selected FDA GCP/Clinical Trial Guidance Documents
    - ICH Guidance Documents
    - GCP/Clinical Trial Notices

6.2 Electronic Records

6.2.1 Controls for Closed Systems

6.2.1.1 Controls for closed systems #1

Requirement:	Persons who used closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine.
Functionality:	System provides procedures which prevent that the signer repudiate the signed record as not genuine.
Function tested:	Procedures that allow the signer ´to repudiate the signed record as not genuine are not available.

6.2.1.2 Controls for closed systems #2

Requirement:	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
Functionality:	System detects invalid or altered records.
Function tested:	Recognition of invalid or altered records is possible.

6.2.1.3 Controls for closed systems #3

Requirement:	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying by the ability of the agency to perform such review and copying of the electronic records.
Functionality:	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any

	questions regarding the ability of the agency to perform such review and copying by the ability of the agency to perform such review and copying of the electronic records.
Function tested:	The system generates accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.

6.2.1.4 Controls for closed systems #4

Requirement:	Protection of records to enable their accurate and ready retrieval throughout the records retention period.
Functionality:	System protects records, enables their accurate and ready retrieval throughout the records retention period.
Function tested:	Records are protected throughout the records retention period. Retrival is possible.

6.2.1.5 Controls for closed systems #5

Requirement:	Limiting system access to authorized individuals.
Functionality:	System allows to define user profile.
Function tested:	Definition of user profile is possible.

6.2.1.6 Controls for closed systems #6

Requirement:	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and action that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be 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.
Functionality:	System provides Audit Trail which records any changes of data.
Function tested:	Audit Trail is available.

6.2.1.7 Controls for closed systems #7

Requirement:	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.
Functionality:	System uses operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Function tested:	System checks to enforce permitted sequencing of steps and events, as appropriate are available.

6.2.1.8 Controls for closed systems #8

Requirement:	Use of authority checks to ensure that only authorized individuals can use the system input or output device, alter a record, or perform the operation at hand.
Functionality:	System executes authority checks.
Function tested:	Authority checks can be executed.

6.2.1.9 Controls for closed systems #9

Requirement:	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.
Functionality:	System executes device (e.g., terminal) checks.
Function tested:	Device checks can be executed.

6.2.1.10 Controls for closed systems #10

Requirement:	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.
Functionality:	Persons who develop, maintain, or use electronic record/electronic signature systems must show the education, training, and experience to perform their assigned tasks.
Function tested:	All persons who develop, maintain, or use electronic record/electronic signature systems have documents that prove their education, training, and experience to perform their assigned tasks.

6.2.1.11 Controls for closed systems #11

Requirement:	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.
Functionality:	System allows establishing written policies which make users responsible for their actions initiated under their electronic signatures.
Function	Written policies are available.

tested:	

6.2.1.12 Controls for closed systems #12

Requirement:	Use of appropriate controls over systems documentation including: • Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. • Revision and change control procedures to maintain an audit trail that document time-sequenced development and modification of systems documentation.
Functionality:	System provides Audit Trail of documentation which records who made changes, what was changed and when a change has been made.
Function tested:	Audit Trail is available.

6.2.2 Signature Manifestation

Requirement:	Signed electronic records shall contain information associated with signing that clearly indicates all of the following: • The printed name of the signer. • The data and time when the signature was executed; and • The meaning (such as review, approval, responsibility, or authorship) associated with the signature.
Functionality:	System provides signature of electronic records.
Function tested:	Electronic signature is available.

6.2.3 Signature Record/Linking

Requirement:	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.
Functionality:	System prevents the falsification of documents by use of electronic signatures.
Function tested:	Falsification of electronic signatures is not possible.

6.3 Electronic Signatures

6.3.1 General Requirements

6.3.1.1 General Requirements #1

Requirement:	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to anyone else.
Functionality:	System assigns unique electronic signatures.
Function tested:	Explicit assignment of electronic signature is possible.

6.3.1.2 General Requirements #2

Requirement:	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.
Functionality:	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.
Function tested:	Organization has verified the identity of the individual.

6.3.1.3 General Requirements #3

Requirement:	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. • The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. • Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.
Functionality:	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.
Function tested:	Persons have certified that their electronic signatures are a legally binding equivalent of the traditional handwritten signatures.

6.3.2 Electronic Signature Components and Controls

6.3.2.1 Electronic Signature Components and Controls #1

Requirement:	Electronic signatures that are not based upon biometric shall: 1. Employ at least two distinct identification components such as an identification code and password. a. When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. b. When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. 2. Be used only by their genuine owners; and 3. Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.
Functionality:	System allows to use electronic signatures in following combinations: 1. If a user executes a series of signings during a single, continuous period of controlled system access the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component 2. When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components 3. Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals
Function tested:	1. First signing can be executed using all electronic signature components; subsequent signings can be executed using at least one electronic signature component 2. Each signing can be executed using all of the electronic signature components 3. Attempted use of an individual's electronic signature by anyone other than its genuine owner has required collaboration of two or more individuals

6.3.2.2 Electronic Signature Components and Controls #2

Requirement:	Electronic signature based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.
Functionality:	System prevents to falsify biometric signatures.

Function tested:	Falsification of biometric signatures is not possible.

6.4 Controls for Identifications Codes and Passwords

6.4.1 Controls for Identifications Codes and Passwords #1

Requirement:	Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.
Functionality:	System prevents that two user gets the same combination of identification code and password.
Function tested:	The allocation of the same combination of identification code and password to two different users is not possible.

6.4.2 Controls for Identifications Codes and Passwords #2

Requirement:	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).
Functionality:	System allow to check identification code and password periodically.
Function tested:	System allow to check identification code and password periodically.

6.4.3 Controls for Identifications Codes and Passwords #3

Requirement:	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.
Functionality:	System allows control of loss management procedures.
Function tested:	Control of loss management procedures is possible.

6.4.4

6.4.5 Controls for Identifications Codes and Passwords #4

Requirement:	Use of transcription safeguards to prevent unauthorized use of passwords and/or attempts at their unauthorized use to the system security unit, as appropriate, to organizational management.

Functionality:	System provide safeguards to prevent the unauthorized use to the system security unit.
Function tested:	Unauthorized access to the system security unit is not possible.

6.4.6 Controls for Identifications Codes and Passwords #5

Requirement:	Initial and periodic testing of devices, such as token or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.
Functionality:	Initial and periodic testing of devices, such as token or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.
Function tested:	Token or cards, that bear or generate identification code or password information function properly and are not altered in an unauthorized manner.

7 FDA Guidance for Industry for Computerized Systems Used in Clinical Trials

As the FDA states, the criteria below address the issues pertaining to computerized systems used to create, modify, maintain, archive, retrieve, or transmit clinical data intended for submission to the FDA. The collected data form the basis for the FDA to decide about the safety and efficacy of new drugs, medical devices, etc. and thus they have high public health significance and thus must fulfil highest standards towards quality and integrity to conform to FDA's regulations.

Therefore the acceptance of data from clinical trials for decision-making purposes depends on the ability to verify the data's quality and integrity during onsite inspections and audits. To be acceptable the data should meet several quality specifications, such as being attributable, original, accurate, contemporaneous, and legible. The following criteria present how those specifications can be satisfied in computerized systems that are being used to create, modify, maintain, archive, retrieve, or transmit clinical data.

The principles in this guidance may be applied where source documents are created

1. in hardcopy and later entered into a computerized system,
2. by direct entry by a human into a computerized system, and
3. automatically by a computerized system.

7.1 General Principles

7.1.1 General Principle #1

Requirement:	The design of a computerized system should ensure that all applicable regulatory requirements for record keeping and record retention in clinical trials are met with the same degree of confidence as is provided with paper systems.
Functionality:	eDocuments have the same degree of confidence which is provided by paper Documents.
Function tested:	System provide the same degree of confidence for eDocuments which is by paper Documents available.

7.1.2 General Principle #2

Requirement:	Any changes to a record required to be maintained should not obscure the original information. The record should clearly indicate that a change was made and clearly provided a means to locate and read the prior information.
Functionality:	Audit Trail should be set up to record who make the changes and which changes has been made.
Function tested:	It is possible to read in Audit Trail report the prior Information after a change was executed.

7.1.3 General Principle #3

Requirement:	Changes to data that are stored on electronic media will always require an audit trail, in accordance with 21 CRF 11.10(e). Documentation should include who made the changes, when, and why they were made.
Functionality:	Audit Trail should be set up to record who makes the changes and which changes have been made.
Function tested:	It is possible to read in an Audit Trail report who made the changes, when, and why they were made.

7.1.4 General Principle #4

Requirement:	Data should be retrievable in such a fashion that all information regarding each individual subject in a study is attributable to that subject.
Functionality:	System allows to lay a new patient and to store all information regarding to this patient under his name.
Function tested:	After a click on the name of a Patient all information regarding to him is displayed.

7.1.5 General Principle #6

Requirement:	Computerized systems should be designed: (1) So that all requirements assigned to these systems in a study protocol are satisfied (e.g., data are recorded in metric units, requirements that the study be blinded); and, (2) to preclude errors in data creation, modification, maintenance, archiving, retrieval, or transmission.
Functionality:	System allows generating a study protocol according to requirements which preclude errors in data creation, modification, maintenance, archiving, retrieval, or transmission.
Function tested:	A study protocol according to requirements can be designed.

7.1.6 General Principle #6

Requirement:	Security measures should be in place to prevent unauthorized access to the data and to the computerized system
Functionality:	System requires password and username to log in.
Function tested:	Password and username requirement message is displayed for log in.

.

7.2 Standard Operating Procedures

7.2.1 Standard Operating Procedure #1

Requirement:	Standard Operating Procedures (SOPs) pertinent to the use of the computerized system should be available on site.
Functionality:	User should define their SOPs.
Function tested:	User-defined SOPs are available on site.

7.2.2 Standard Operating Procedure #2

Requirement:	SOPs should be established for, but not limited to: • System Setup/installation • Data Collection and Handling • System Maintenance • Data Backup, Recovery, and Contingency Plans • Security • Change Control
Functionality:	SOPs should be defined for all task.
Function tested:	Comprehensive defined SOPs are available.

7.3 Data Entry

7.3.1 Electronic Signature

7.3.1.1 Electronic Signature #1

Requirement:	To ensure that individuals have the authority to proceed with data entry system should be designed so that individuals need to enter electronic signatures, such as combined identification codes/passwords or biometric-based electronic signatures, at the start of a data entry session.
Functionality:	System should requires combined identification codes/passwords or biometric-based electronic signatures to log in.
Function tested:	System requires electronic signature to log in.

7.3.1.2 Electronic Signature #2

Requirement:	The data entry system should also be designed to ensure attributability. Therefore, each entry to an electronic signature of the individual making that entry. However, this does not necessarily mean a separate electronic signature may cover multiple entries or changes.

	a. The printed name of the individual who enters data should be displayed by the data entry screen throughout the data entry session. This is intended to preclude the possibility of a different individual inadvertently entering data under someone else's name. b. If the name displayed by the screen during a data entry session is not that of the person entering the data, then that individual should log on under his or her own name before continuing.
Functionality:	System should require electronic signature of user and should display the name of user which edit eDocuments.
Function tested:	System displays continued name of user.

7.3.1.3 Electronic Signature #3

Requirement:	Individuals should only work under their own passwords or other access keys and should not share these with others. Individuals should not log on to the system in order to provide another person access to the system.
Functionality:	System allows to design an explicit user ID.
Function tested:	Users can work only with an explicit user ID.

7.3.1.4 Electronic Signature #4

Requirement:	Passwords or other access keys should be changed at established intervals.
Functionality:	System allows to change access keys at established interval.
Function tested:	It is possible to change access keys at established interval.

7.3.1.5 Electronic Signature #5

Requirement:	When someone leaves a workstation, the person should log off the system. Failing this, an automatic log off may be appropriate for long idle periods. For short period of inactivity, there should be some kind of automatic protection against unauthorized data entry. An example could be an automatic screen saver that prevents data entry until a password is entered.
Functionality:	System should log off automatically after long idle periods. For short period of inactivity, system requires password to enter data.
Function tested:	After long idle periods occurs log off automatically and for short periods of inactivity, system requires password to enter data.

7.3.2 Audit Trail

7.3.2.1 Audit Trail #1

Requirement:	Section 21 CRF 11.10(e) requires persons who use electronic record systems to maintain an audit trail as one of the procedures to protect the authenticity, integrity, and, when appropriate, the confidentiality of electronic records. a. persons must use secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. A record is created when it is saved to durable media, as described under "commit" in Section II, definitions. b. Audit trails must be retained for a period at least as long as that required for the subject electronic records (e.g., the study data record to which they pertain) and must be available for agency review and copying.
Functionality:	System provides Audit Trail which records who makes changes at data when were these did and which changes had been executed.
Function tested:	Audit trail report shows changes that were made.

7.3.2.2 Audit Trail #2

Requirement:	Personnel who creates, modifies, or deletes electronic records should not be able to modify the audit trails.
Functionality:	Users have not access to Audit Trail and they cannot execute any changes in Audit Trail.
Function tested:	It is not possible to access at Audit Trail.

7.3.2.3 Audit Trail #3

Requirement:	Clinical investigators should retain either the original or a certified copy of audit trails.
Functionality:	System allows to provide original and copy of audit trails for auditor purposes.
Function tested:	Original and copy of audit trails are available.

7.3.2.4 Audit Trail #4

Requirement:	FDA personnel should be able to read audit trails both at the study site and at any other location where associated electronic study records are

	maintained.
Functionality:	System allows to provide Audit Trail reports in network which maintain electronic study records.
Function tested:	Audit Trail reports are to each site of network which maintain electronic study records are available.

7.3.2.5 Audit Trail #5

Requirement:	Audit trails should be created incrementally, in chronological order, and in a manner that does not allow new audit trail information to overwrite existing data in violation of §11.10(e).
Functionality:	System provides Audit Trail that records changes chronologically and prevent that new audit trail information to overwrite existing data.
Function tested:	Audit Trail with chronological record function is available.

7.3.3 Date/Time Stamps

7.3.3.1 Date/Time Stamp #1

Requirement:	Controls should be in place to ensure that the system's date and time are correct.
Functionality:	System maintains mechanism that checks and provide the correct time.
Function tested:	Checks for correct time stamps are available.

7.3.3.2 Date/Time Stamp #2

Requirement:	The ability to change the data or time should be limited to authorized personnel and such personnel should be notified if a system date or time discrepancy is detected. Changes to date or time should be documented.
Functionality:	System allows to define that only system-administrators have the right to change data or time.
Function tested:	It is possible to ensure that only system-administrator can change time and date.

7.3.3.3 Date/Time Stamp #3

Requirement:	Dates and time are to be local to the activity being documented an should include the year, month, day, hour, and minute. The agency encourages establishments to synchronize systems to the date and time provided by

	trusted third parties.
Functionality:	System shows local time in year, month, day, hour, and minute.
Function tested:	eDocuments show local time in year, month, day, hour and minute.

7.3.3.4 Date/Time Stamp #4

Requirement:	Clinical study computerized systems will likely be used in multi-centre trails, perhaps located in different time zones. Calculation of the local time stamp may be derived in such cases from a remote server located in a different time zone.
Functionality:	Calculation of local time stamp in different time zones in multi-centre trails is possible.
Function tested:	Calculation of local time stamp in different time zones in multi-centre trails is possible.

7.4 System Features

7.4.1 System Used for Direct Entry of Data Should Include Features that Will Facilitate the Collection of Quality Data

7.4.1.1 System Used for Direct Entry of Data… #1

Requirement:	Prompts, flags, or other help features within the computerized system should be used to encourage consistent use of clinical terminology and to alert the user to data that are out of acceptable range. Features that automatically enter data into a field when that field is bypassed should not be used.
Functionality:	Prompts, flags, or other help features within the computerized system are available to warn if data are out of acceptable range.
Function tested:	If data are out of acceptable range there will be are out of acceptable range to warn.

7.4.1.2 System Used for Direct Entry of Data… #2

Requirement:	Electronic patient diaries and e-CRFs should be designed to allow users to make annotations. Annotations add to data quality by allowing ad hoc information to be captured. This information may be valuable in the event of an adverse reaction or unexpected result. The record should clearly indicate who recorded the annotations and when (date and time).
Functionality:	System allows to create electronic patient diaries and e-CRFs.
Function tested:	It is possible to create electronic patient diaries and e-CRFs that allow to make annotations.

7.4.1.3 System Used for Direct Entry of Data… #3

Requirement:	Systems used for direct entry of data should be designed to include features that will facilitate the inspection and review of data. Data tags (e.g., different colour, different font, flags) should be to indicate which data have been changed or deleted, as documented in the audit trail.
Functionality:	System allows to use Data tags that show data has been edited.
Function tested:	Data tags that show data as being edited are available.

7.4.2 Retrieval of Data

7.4.2.1 Retrieval of Data #1

Requirement:	Recognizing that computer products may be discontinued or supplanted by newer (possibly incompatible) systems, it is nonetheless vital that sponsors retain the ability to retrieve and review the data recorded by the older systems. This may be achieved by maintaining support for the older systems or transcribing data to the new systems.
Functionality:	System allows to retrieve and review the data recorded by older systems.
Function tested:	System allows to retrieve and review the data recorded by older systems.

7.4.2.2 Retrieval of Data #2

Requirement:	When migrating to newer systems, it is important to generate accurate and complete copies of study data and collateral information relevant to data integrity. This information would include, for example, audit trails and computational methods used to derive the data. Any data retrieval software, script, or query logic used for the purpose of manipulating, querying, or extracting data for report generating purposes should be documented and maintained for the life of the report. The transcription process needs to be validated.
Functionality:	System allows to generate accurate and complete copies of study data and collateral information relevant to data integrity.
Function tested:	Generation of accurate and complete copies of study data and collateral information relevant to data integrity is possible.

7.4.3 Reconstruction of Study

Requirement:	FDA expects to be able to reconstruct a study. This applies not only to the data, but also how the data were obtained or managed. Therefore, all versions of application software, operating systems, and software

	development tools involved in processing of data or records should be available as long as data or records associated with these versions are required to be retained. Sponsors may retain these themselves or may contract for the vendors to retain the ability to run (but not necessarily support) the software. Although FDA expects sponsors or vendors to retain the ability to run older versions of software, the agency acknowledges that, in some cases, it will be difficult for sponsors and vendors to run older computerized systems.
Functionality:	System allows to reconstruct a study.
Function tested:	Reconstruction of a study is possible.

7.5 Security

7.5.1 Physical Security

7.5.1.1 Physical Security #1

Requirement:	In additional to internal safeguards built into the system, external safeguard should be in place to ensure that access to the computerized system and to the data is restricted to authorized personnel.
Functionality:	System allows to install external safeguards.
Function tested:	External safeguards are in place.

7.5.1.2 Physical Security #2

Requirement:	Staff should be thoroughly aware of system security measures and the importance of limiting access to authorized personnel.
Functionality:	System allows to make administrator-defined access.
Function tested:	It is possible to allow administrator-defined access.

7.5.1.3 Physical Security #3

Requirement:	SOPs should be in place for handling and storage in the system to prevent unauthorized access.
Functionality:	System allows to store SOPs.
Function tested:	SOPs are available and can be stored.

7.5.2 Logical Security

7.5.2.1 Logical Security #1

Requirement:	Access to data at the clinical site should be restricted and monitored through the system's software with its required log-on, security procedures, and audit trail. The data should not be altered, browsed, queried, or reported via external software applications that do not enter through the protective system software.
Functionality:	System provide Audit Trail which records changes at clinical data and prevent unauthorized external access.
Function tested:	Audit Trail is Available and it is not possible to access the system unauthorized.

7.5.2.2 Logical Security #2

Requirement:	There should be a cumulative record that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges. The record should be in the study documentation accessible at the site.
Functionality:	System provides a record that shows for any point in time, the names of authorized personnel, their titles, and a description of their access privileges.
Function tested:	A record with user data available.

7.5.2.3 Logical Security #3

Requirement:	If a sponsor supplies computerized systems exclusively for clinical trials, the systems should remain dedicated to the purpose for which they were intended and validated.
Functionality:	System prevents the use of other purposes than clinical trials.
Function tested:	System prevents the use of other purposes than clinical trials.

7.5.2.4 Logical Security #4

Requirement:	If a computerized system being used for the clinical study is part of a system normally used for other purposes, efforts should be made to ensure that the study software is logically and physically isolated as necessary to preclude unintended interaction with non-study software. If any of the software programs are changed the system should be evaluated to determine the effect of the changes on logical security.

Functionality:	If a computerized system being used for the clinical study is part of a system normally used for other purposes, efforts should be made to ensure that the study software is logically and physically isolated as necessary to preclude unintended interaction with non-study software.
Function tested:	It is possible to isolate logically und physically study software from non-study software.

7.5.2.5 Logical Security #5

Requirement:	Controls should be in place to prevent, detect, and mitigate effects of computer viruses on study data and software.
Functionality:	System provides antiviral programs.
Function tested:	Antiviral programs are available.

7.6 System Dependability

7.6.1 System Dependability #1

Requirement:	The sponsor should ensure and document the computerized systems conform to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance.
Functionality:	System fulfilled requirements.
Function tested:	System fulfilled requirements.

7.6.2 System Dependability #2

Requirement:	System documentation should be readily available at the site where clinical trials are conducted. Such documentation should provide an overall description of computerized systems and the relationship of hardware, software, and physical environment.
Functionality:	System documentation should be readily available at the site where clinical trials are conducted.
Function tested:	System documentation is available.

7.6.3 System Dependability #3

Requirement:	FDA may inspect documentation, possessed by a regulated company, that demonstrates validation of software. The study sponsor is responsible, if

	requested, for making such documentation available at the time of inspection at the site where software is used. Clinical investigators are not generally responsible for validation unless they originated or modified software.
Functionality:	FDA may inspect validation documentation.
Function tested:	Documents of validation of software are available for inspection.

7.6.4 System Dependability #4

Requirement:	For software purchased off-the-shelf, most of the validation should have been done by the company that wrote the software. The sponsor or contact research organization should have documentation (either original validation documents or on-site vendor, and should have itself performed functional testing (e.g., by use of test data sets) and researched known software limitations, problems, and defect corrections.
Functionality:	Validation Documents provided by the company and executed by sponsor are available
Function tested:	Validation Documents provided by the company and executed by sponsor are available

7.6.5 System Dependability #5

Requirement:	In the special case of database and spreadsheet software that is (1) purchased off-the-shelf, (2) designed for and widely used for general purposes, (3) unmodified, and (4) not being used for direct entry of data, the sponsor or contract research organization may not have documentation of design level validation. However, the sponsor or contract research organization should have itself performed functional testing (e.g., by use of test data set) and researched known software limitations, problems, and defect correction.
Functionality:	Validation Documents for off-the-shelf software were created by functional testing.
Function tested:	Validation Documents for off-the-shelf software are available.

7.6.6 System Dependability #6

Requirement:	Written design specification that describes what the software is intended to do and how intended to do it.
Functionality:	Written design specification were created.
Function tested:	Written design specification are available.

7.6.7 System Dependability #7

Requirement:	A written test plan based on the design specification, including both structural and functional analysis; and, Test results and an evaluation of how these results demonstrate that the predetermined design specification has been met.
Functionality:	A written test plan based on the design specification is available.
Function tested:	A written test plan based on the design specification was used for validation.

7.6.8 System Dependability #8

Requirement:	Written procedures should be in place to ensure that changes to the computerized system such as software upgrades, equipment or component replacement, or new instrumentation will maintain the integrity of the data or the integrity of protocols.
Functionality:	Written procedures which ensure the integrity of data or protocols after any changes are in place.
Function tested:	System shows integrity of data or protocols after executed changes.

7.6.9 System Dependability #9

Requirement:	The impact of any changes to the system should be evaluated and a decision made regarding the need to revalidate. Revalidation should be performed for changes that exceed operational limits or design specifications.
Functionality:	It is possible to execute revalidation for changes that exceed operational limits or design specifications.
Function tested:	Revalidation for changes that exceeded operational limits or design specifications can be executed.

7.6.10 System Dependability #10

Requirement:	All changes to the system should be documented.
Functionality:	All changes to the system should be documented.
Function tested:	Documents for all executed changes are available.

7.7 System Controls

7.7.1 System Controls #1

Requirement:	Measures should be in place to ensure that versions of the software used to generate, collect, maintain, and transmit data are the versions that are stated in the systems documentation.
Functionality:	System documentation maintains the versions that are stated in the systems.
Function tested:	System version management exists.

7.7.2 System Controls #2

Requirement:	Written procedures should describe contingency plans for continuing the study by alternate means in the event of failure of the computerized system.
Functionality:	Written procedures should describe contingency plans for continuing the study by alternate means in the event of failure of the computerized system.
Function tested:	Contingency plans for continuing the study by alternate means in the event of failure of the computerized system are available.

7.7.3 System Controls #3

Requirement:	Backup and recovery procedures should be clearly outlined in the SOPs and be sufficient to protect against data loss. Records should be backed up regularly in a way that would prevent a catastrophic loss and ensure the quality and integrity of the data.
Functionality:	Backup and recovery procedures should be clearly outlined in SOPs and be sufficient to protect system against data loss.
Function tested:	Backup and recovery procedures are available.

7.7.4 System Controls #4

Requirement:	Backup records should be stored at a secure location specified in the SOPs. Storage is typically offsite or in a building separate from the original records.
Functionality:	Backup storage is typically offsite or in a building separate from the original records.
Function tested:	Backup storage is offsite or in a building separate.

7.7.5 System Controls #5

Requirement:	Backup and recovery logs should be maintained to facilitate an assessment of the nature and scope of data loss resulting from a system failure.
Functionality:	System allows maintaining backup and recovery logs.
Function tested:	Backup and recovery logs are maintained.

7.8 Training of Personnel

7.8.1 Training of Personnel #1

Requirement:	Each person who enters or processes data should have the education, training, and experience or any combination thereof necessary to perform the assigned functions.
Functionality:	Personnel should be trained to execute assigned functions.
Function tested:	Personnel is trained to execute assigned functions.

7.8.2 Training of Personnel #2

Requirement:	Individuals responsible for monitoring the trial should have education, training, and experience in the use of the computerized system necessary to adequately monitor the trial.
Functionality:	Personnel should be trained in computerized system to monitor the trial.
Function tested:	Personnel is trained in the use of computerized system to monitor the trial.

7.8.3 Training of Personnel #3

Requirement:	Training should be provided to individuals in the specific operations that they are to perform.
Functionality:	Training should be provided to individuals in the specific operations that they have to perform.
Function tested:	Training should be provided to individuals in the specific operations that they have to perform.

7.8.4 Training of Personnel #4

Requirement:	Training should be conducted by qualified individuals on a continuing basis, as needed, to ensure familiarly with the computerized system during the course of the study.
Functionality:	Training should be conducted by qualified individuals on a continuing basis, as needed, to ensure familiarly with the computerized system during the course of the study.
Function tested:	Training is conducted by qualified individuals on a continuing basis, to ensure familiarly with the computerized system during the course of the study.

7.8.5 Training of Personnel #5

Requirement:	Employee education, training, and experience should be documented.
Functionality:	Employee education, training, and experience should be documented.
Function tested:	Employee education, training, and experience documents are available.

7.9 Record Inspection

7.9.1 Record Inspection #1

Requirement:	FDA may inspect all records that are intended to support submissions to the Agency, regardless of how they were created or maintained. Therefore, systems should be able to generate accurate and complete copies of records in both human readable and electronic from suitable for inspection, review, and copying by the Agency. Persons should contact the Agency if there is any doubt about what file formats and media the Agency can read and copy.
Functionality:	Systems can generate accurate and complete copies of records in both human readable and electronic from suitable for inspection, review, and copying by the agency.
Function tested:	System generates accurate and complete copies of records in both human readable and electronic from suitable for inspection by the agency.

7.9.2 Record Inspection #2

Requirement:	The sponsor should be able to provide hardware and software as necessary for FDA personnel to inspect the electronic documents and audit trail at the site where an FDA inspection is taking place.
Functionality:	The sponsor should be able to provide hardware and software as necessary for FDA personnel to inspect the electronic documents and audit trail at the

	site where an FDA inspection is taking place.
Function tested:	Necessary hardware and software is provided for FDA inspection.

7.10 Certification of Electronic Signatures

Requirement:	As required by 21 CRF 11.100(c), persons using electronic signatures to meet an FDA signature requirement shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be legally binding equivalent of traditional handwritten signatures.
Functionality:	As required by 21 CRF 11.100(c), persons using electronic signatures to meet an FDA signature requirement shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be a legally binding equivalent of traditional handwritten signatures.
Function tested:	Persons using electronic signatures have certified to the agency that the electronic signatures are intended to be legally binding.

8 Applicability for ObTiMA and DoctorEye[10]

8.1 ObTiMA

ObTiMA (http://obtima.org/) is an ontology-based clinical trial management system intended to support clinicians in both designing and conducting clinical trials[11]. Thus, ObTiMA will enable not only specialized data management stuff to create CRFs, but trial investigators can assemble proper CRFs for their planned clinical trial. The design phase is facilitated by the Trial Builder in which different aspects of a clinical trial can be specified. For example, the outline and metadata of a trial or administrative data, but also treatment plans for guiding clinicians through individual patient treatments including surgery or chemotherapy can be defined with all necessary information. The particular treatment order can be setup on a graphic timeline as well as treatment stratifications and randomizations can be applied. A CRF can be connected to each treatment step to collect documentation data at the right time point. Functionalities:

- Roles and Rights Management
- Audit trail
- Pseudonymization
- User/Facility Management
- Data Export
- Reporting

The ontology-based creation of CRFs in the Trial Builder is one of ObTiMA's major functionalities and highlights (see Fig. 1). A graphical user interface allows the definition of content, the navigation, and the definition of layout of CRFs. The resulting descriptions are based on concepts of the ACGT Master Ontology for each CRF item along with metadata (data type and measurement unit) and used for the automatic setup of the trial database. An application-specific, simplified view of the ontology is given showing only its relevant portions in a clinician-friendly way. When an item has been created based on a concept, its attributes are determined automatically, e.g., label, data type or answer possibilities but can be manually adopted.

Often clinical trials collect similar or equal data. Therefore, it is possible to store components of CRFs in a repository as templates (CRF repository). When implementing a clinical trial, CRF templates can either be directly reused or can be quickly created by assembling existing CRF components with newly created CRF components. This procedure has the advantage that it enhances the standardization of CRFs. The second major component of ObTiMA is the patient data management. It is automatically implemented based on the items defined in the Trial Builder. It guides the clinicians through the treatment of the individual patients according to the corresponding treatment plan. The trial database is automatically derived from the ontology-based CRF definitions. Thus, given appropriate rights are given, the database can then also be accessed by other trials or applications through using a semantic mediation service based on the ontology.

ObTiMA offers different modules to support clinical trials. Besides the above described basic components a DICOM server and DICOM viewer (for imaging in clinical trials), a SAE and SUSAR reporting tool and a consultation tool will be integrated. Reporting will be done according to GCP criteria. The consultation tool will store all consultations in a standardized way in the trial database. ObTiMA fulfils GCP criteria, including the availability of an Audit

[10] The content of this section i staken from deliverable D5.5 for now but it will be greatly expanded during the course oft he project as we learn bette runderstand how the criteria described in this deliverable can best be applied to ObTiMA and DrEye.

[11] Holger Stenzhorn, Fatima Schera, Micke Kuwahara, Norbert Graf: ObTiMA - Ontology based Trial Management System for ACGT. ACGT No 14, 2010

Trail and a pseudonymisation tool. Pseudonymisation of private data is done according to specified roles and rights assigned to users of ObTiMA. Data Management in personalised clinical trials covers the collection and validation of a multitude of clinical and genomic data with the goal to answer research questions and to preserve them for future scientific investigations.

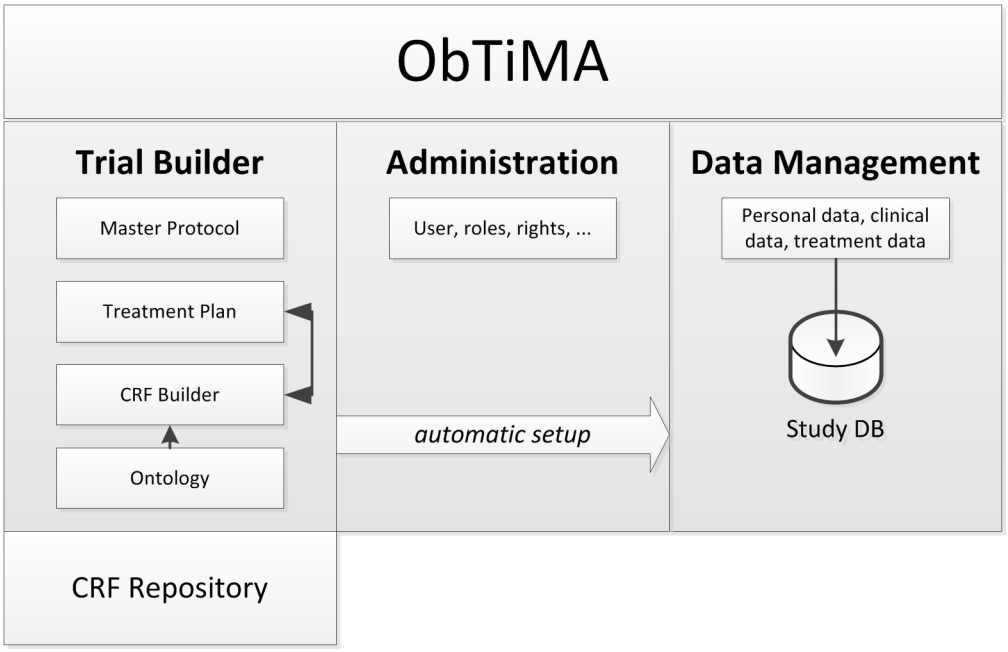

Fig. 1: ObTiMA architecture

Current CDMS often still lack sufficient metadata support and are not semantically interoperable. Therefore, ObTiMA was developed to allow designing trials according to investigator's needs and for this purpose to include a clinical trial ontology. The development of ObTiMA did start as part of the EU project ACGT (Advancing Clinico-Genomic Trials on Cancer) to create an open, semantic and grid-based data management infrastructure for scientists in post-genomic clinical trials in cancer research. The development continued with the project ContraCancrum extending the focus of ObTiMA the integration into a platform for simulating tumour development and response to therapeutic modalities. In p-medicine, the development of ObTiMA will be focused on the demands of personalized clinical trials. During the development of ObTiMA several guidelines for GCP criteria have already been considered:

- 21 CFR Part 11
- Orlando Lopez: Complete Guide to International Computer Validation Compliance for the Pharmaceutical Industry/; ISBN 0-8493-2243-X
- Guidance for Industry. Computerized Systems Used in Clinical Investigations
- Installation Qualification, Operational Qualification and Performance Qualification documentation
- ACDM/PSI Working Party, Computer Systems Validation in Clinical Research

For clinical trial data input, data is entered by investigators manually data for a trial. It will be possible to import data into ObTiMA via CDISC standard. For the export of data (output data) export of collected clinical trial data via CDISC is possible. Long-term data storage of exported trials data for study archiving is supported.

8.1.1 System Components

8.1.1.1 Trial Builder

The Trial Builder represents one of the ObTiMA's two main components (Fig. 1) and enables the investigator to specify the clinical trial. The trial outline and clinical trial metadata can be defined in a master protocol based on templates for describing the trial goals and its administrative data, like start or end date. Treatment plans can be graphically designed to guide clinicians through the treatment of individual patients and particular treatment events, such as chemotherapy or surgery, can be defined with all necessary information. To create a CRF The investigator selects terms from the ontology:

8.1.1.2 CRF Repository

Applying the Master Ontology allows the usage of standardized concepts when creating the CRF. CRF design will be further improved by the partial or complete reuse of existing CRF items in case similar data is collected. The unified CRF Repository is crucial part of ObTiMA. This repository allows the storage and retrieval of entire ontology-based CRFs as well as CRF items or components for reuse.

8.1.1.3 Patient Data Management System (PDMS)

The PDMS is automatically implemented based on the master protocol and the trial CRFs designed in the Trial Builder. The PDMS guides the clinicians through the treatment of patients according to treatment plans. For this purpose it provides a graphical user interface to complete CRF at the correct time point.

8.1.1.4 Data Export

As a tool for personalized clinical trials it is important that ObTiMA can be integrated with other applications. ObTiMA is capable to interface with other existing CTMS and to be able to exchange data in a standardised format. ObTiMA is able to import and export trial metadata, CRF descriptions and patient data through an extended version of the CDISC ODM format.

8.1.1.5 Biomaterial Manager

Biobank access and biomaterial management is integrated into ObTiMA (cf. Fig. 2). The trial biomaterial manager is been developed as a component of the trial management system ObTiMA to enable management of biomaterial data and sharing selected biomaterial data in clinical trials. The trial biomaterial manager will provide an import service that enables users to import excel files with existing biomaterial data. Biobank data can be uploaded to p-BioSPRE (upload services provided). The trial biomaterial manager/ObTiMA system integrates push services that are able to push selected biomaterial data into a data warehouse. Potential users are clinicians and biobank owners.

p-BioSPRE (p-medicine Biomaterial Search and Project Request Engine) is a meta-biobank that provides researchers with the possibility to search for and request biomaterials. p-BioSPRE will be based on the CRIP meta-biobank concept (http://www.crip.fraunhofer.de/) including a web application. It will be integrated into the p-medicine portal. Potential users are mainly researchers. p-BioSPRE will be used as centralized Biobank Access Tool and will use anonymized data only.

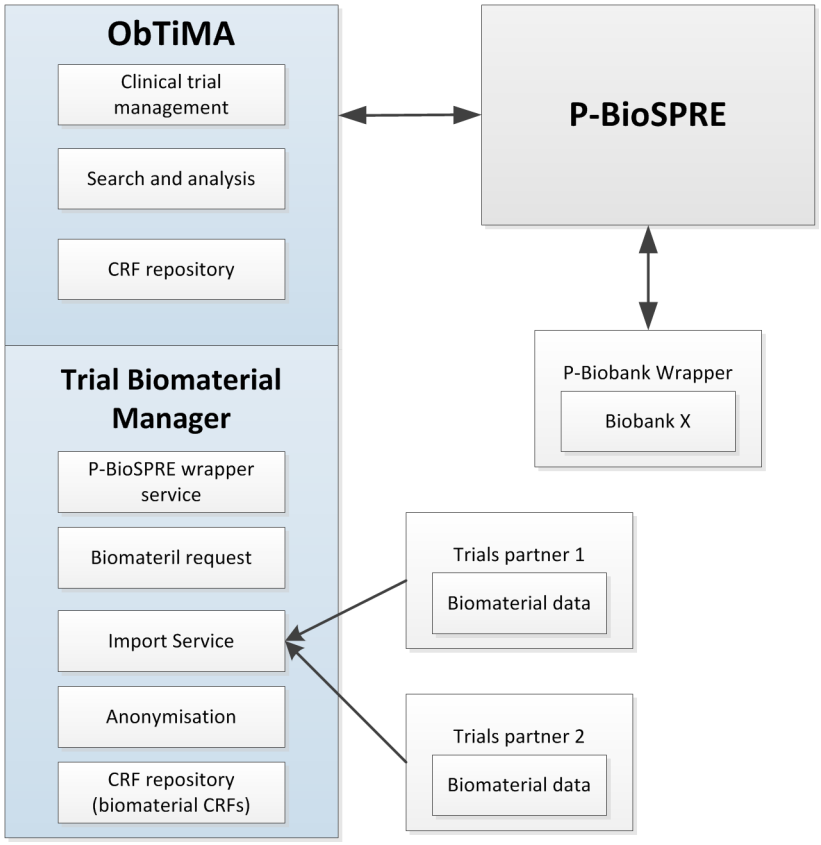

Fig. 2: Integrated biobank access in ObTiMA

8.1.1.6 Additional modules

ObTiMA contains several functions for managing the multitude of institutions, researchers, and patients usually participating in clinical trials. A fine grained security architecture has been implemented to handle the rights and roles that can be attached to the system's users in order to guarantee that they can only perform the tasks which they are fully authorized for. It is indispensable for ObTiMA, as a system holding real patient data, to securely store all of the data which could possibly identify some patient to non-authorized persons in pseudonymized and encrypted form. To foster security even more, such personal data is physically separated from the actual clinical research data through the use of two distinct database servers: One server holds the database for storing the personal data of the patients, such as their names and addresses (which must never be shared, e.g., via the Semantic Mediator). The protection of this database strictly follows all current legal regulations for data protection in clinical environments. The other server hosts the database that contains the actual research data collected in a clinical trial (through the use of the CRFs). It is possible within the Trial Builder to mark certain CRF items as personal which results in this data being stored in the trial database. For the management of pharmacovigilance and serious adverse reporting of SAEs/SUSARs a special module enabling SAE data entry and logging, tracking, coding, and case processing for ObTiMA will be developed.

8.1.2 Regulatory issues

Because ObTiMA will be used as a CDMS in clinical trials following regulations and guidelines apply:

Regulations		Guidance
international/US	European	guidelines
CPMP/ICH/135/95	2001/20/EC	FDA Guidance: Computerized Systems
21 CFR Part 11	2005/28/EC	ICH guidelines
HIPAA	GMP Annex 11	ISO 27001: Information Security
Code of Federal Regulations	95/46/EC	PIC/S, GAMP
	2002/58/EC	GCP reflection paper on electronic source
	ENTR/F/2/SF/dn	ECRIN Standard (DM part)

8.2 DrEye

DrEye is a DICOM viewer with a flexible annotation platform for quick and precise identification and delineation of tumours in medical images. The design of the platform is clinically driven in order to ensure that the clinician can efficiently and intuitively annotate large number of 3D tomographic datasets. Both manual and well-known semi-automatic segmentation techniques are available in the platform allowing clinician to annotate multiple regions of interest at the same session. Additionally, it includes contour drawing, refinement and labelling tools that can effectively assist in the delineation of tumours. Furthermore, segmented tumour regions can be annotated, labelled, deleted, added and redefined. The platform has been tested over several MRI datasets to assess usability, extensibility and robustness with promising results.

A module for the management of the DICOM transfer is developed. Input data come from a PACS server used as standard DICOM storage solution. Interaction is possible with a data warehouse. The solution for DICOM transfer is based on dcm4che (http://www.dcm4che.org/) a collection of open source applications and utilities for healthcare. These applications have been developed in the Java programming language for performance and portability. At the core of the dcm4che project is a robust implementation of the DICOM standard and the dcm4che DICOM toolkit is already used in many production applications across the world. Acting as an archive, dcm4chee is able to store any type of DICOM object to standard file systems, with compression if necessary. GCP compliance of data management and quality control is important for imaging solutions. The link between images and data that is extracted from them should be maintained during the clinical trial. Automated and standardized processes should be applied for image management and quality control. For example, automated checks conducted on imaging parameters, checks of image quality. Automatic edit checks on data should be performed during the entire data collection and amendment process. A seamless interoperability between the imaging solution the and the CDMS should be maintained.

8.2.1 Regulatory Issues

Because DrEye will be used for diagnosis in clinical trials following regulations and guidelines apply. As a tool that is used for diagnosis medical device regulations are relevant.

Regulations	Guidance

International/US	European	Guidelines
CPMP/ICH/135/95	2001/20/EC	FDA Guidance: Computerized Systems
21 CFR Part 11	2005/28/EC	ICH guidelines
HIPAA	GMP Annex 11	ISO 27001: Information Security
Code of Federal Regulations	95/46/EC	PIC/S, GAMP
EN ISO 14155:2011	2007/47/EG	FDA Guidance –Clinical Trial Imaging Endpoints
CFR regulations concerning medical devices		

Appendix 1 – Abbreviations and Acronyms

GCP	Good Clinical Practice
ObTiMA	Ontology-based Trial Management Application
QM	Quality Management
SOP	Standard Operating Procedure
SVMP	System Validation Master Plan

Appendix 2 – Definitions

The following definitions are taken from the section 1 (Glossary) of the Note for guidance on Good Clinical Practice (CPMP/ICH/135/95)[12]:

Adverse Drug Reaction (ADR)

In the pre-approval clinical experience with a new medicinal product or its new usages, particularly as the therapeutic dose(s) may not be established: all noxious and unintended responses to a medicinal product related to any dose should be considered adverse drug reactions. The phrase responses to a medicinal product means that a causal relationship between a medicinal product and an adverse event is at least a reasonable possibility, i.e. the relationship cannot be ruled out.

Adverse Event (AE)

Any untoward medical occurrence in a patient or clinical investigation subject administered a pharmaceutical product and which does not necessarily have a causal relationship with this treatment. An adverse event (AE) can therefore be any unfavourable and unintended sign (including an abnormal laboratory finding), symptom, or disease temporally associated with the use of a medicinal (investigational) product, whether or not related to the medicinal (investigational) product (see the ICH Guideline for Clinical Safety Data Management: Definitions and Standards for Expedited Reporting).

Applicable Regulatory Requirement(s)

Any law(s) and regulation(s) addressing the conduct of clinical trials of investigational products.

Approval (in relation to Institutional Review Boards)

The affirmative decision of the IRB that the clinical trial has been reviewed and may be conducted at the institution site within the constraints set forth by the IRB, the institution, Good Clinical Practice (GCP), and the applicable regulatory requirements.

Audit

A systematic and independent examination of trial related activities and documents to determine whether the evaluated trial related activities were conducted, and the data were recorded, analyzed and accurately reported according to the protocol, sponsor's standard operating procedures (SOPs), Good Clinical Practice (GCP), and the applicable regulatory requirement(s).

Audit Certificate

A declaration of confirmation by the auditor that an audit has taken place.

[12] http://www.ema.europa.eu/ema/pages/includes/document/open_document.jsp?webContentId=WC500002874

Audit Report

A written evaluation by the sponsor's auditor of the results of the audit.

Audit Trail

Documentation that allows reconstruction of the course of events.

Blinding/Masking

A procedure in which one or more parties to the trial are kept unaware of the treatment assignment(s). Single-blinding usually refers to the subject(s) being unaware, and double-blinding usually refers to the subject(s), investigator(s), monitor, and, in some cases, data analyst(s) being unaware of the treatment assignment(s).

Case Report Form (CRF)

A printed, optical, or electronic document designed to record all of the protocol required information to be reported to the sponsor on each trial subject.

Clinical Trial/Study

Any investigation in human subjects intended to discover or verify the clinical, pharmacological and/or other pharmacodynamic effects of an investigational product(s), and/or to identify any adverse reactions to an investigational product(s), and/or to study absorption, distribution, metabolism, and excretion of an investigational product(s) with the object of ascertaining its safety and/or efficacy. The terms clinical trial and clinical study are synonymous.

Clinical Trial/Study Report

A written description of a trial/study of any therapeutic, prophylactic, or diagnostic agent conducted in human subjects, in which the clinical and statistical description, presentations, and analyses are fully integrated into a single report (see the ICH Guideline for Structure and Content of Clinical Study Reports).

Comparator (Product)

An investigational or marketed product (i.e., active control), or placebo, used as a reference in a clinical trial.

Compliance (in relation to trials)

Adherence to all the trial-related requirements, Good Clinical Practice (GCP) requirements, and the applicable regulatory requirements.

Confidentiality

Prevention of disclosure, to other than authorized individuals, of a sponsor's proprietary information or of a subject's identity.

Contract

A written, dated, and signed agreement between two or more involved parties that sets out any arrangements on delegation and distribution of tasks and obligations and, if appropriate, on financial matters. The protocol may serve as the basis of a contract.

Coordinating Committee

A committee that a sponsor may organize to coordinate the conduct of a multicentre trial.

Coordinating Investigator

An investigator assigned the responsibility for the coordination of investigators at different centres participating in a multicentre trial.

Contract Research Organization (CRO)

A person or an organization (commercial, academic, or other) contracted by the sponsor to perform one or more of a sponsor's trial-related duties and functions.

Direct Access

Permission to examine, analyze, verify, and reproduce any records and reports that are important to evaluation of a clinical trial. Any party (e.g., domestic and foreign regulatory authorities, sponsor's monitors and auditors) with direct access should take all reasonable precautions within the constraints of the applicable regulatory requirement(s) to maintain the confidentiality of subjects' identities and sponsorís proprietary information.

Documentation

All records, in any form (including, but not limited to, written, electronic, magnetic, and optical records, and scans, x-rays, and electrocardiograms) that describe or record the methods, conduct, and/or results of a trial, the factors affecting a trial, and the actions taken.

Essential Documents

Documents which individually and collectively permit evaluation of the conduct of a study and the quality of the data produced

Good Clinical Practice (GCP)

A standard for the design, conduct, performance, monitoring, auditing, recording, analyses, and reporting of clinical trials that provides assurance that the data and reported results are credible and accurate, and that the rights, integrity, and confidentiality of trial subjects are protected.

Independent Data-Monitoring Committee (IDMC) (Data and Safety Monitoring Board, Monitoring Committee, Data Monitoring Committee)

An independent data-monitoring committee that may be established by the sponsor to assess at intervals the progress of a clinical trial, the safety data, and the critical efficacy endpoints, and to recommend to the sponsor whether to continue, modify, or stop a trial.

Impartial Witness

A person, who is independent of the trial, who cannot be unfairly influenced by people involved with the trial, who attends the informed consent process if the subject or the subjectís legally acceptable representative cannot read, and who reads the informed consent form and any other written information supplied to the subject.

Independent Ethics Committee (IEC)

An independent body (a review board or a committee, institutional, regional, national, or supranational), constituted of medical professionals and non-medical members, whose responsibility it is to ensure the protection of the rights, safety and well-being of human subjects involved in a trial and to provide public assurance of that protection, by, among other things, reviewing and approving/providing favourable opinion on, the trial protocol, the suitability of the investigator(s), facilities, and the methods and material to be used in obtaining and documenting informed consent of the trial subjects.

The legal status, composition, function, operations and regulatory requirements pertaining to Independent Ethics Committees may differ among countries, but should allow the Independent Ethics Committee to act in agreement with GCP as described in this guideline.

Informed Consent

A process by which a subject voluntarily confirms his or her willingness to participate in a particular trial, after having been informed of all aspects of the trial that are relevant to the subject's decision to participate. Informed consent is documented by means of a written, signed and dated informed consent form.

Inspection

The act by a regulatory authority(ies) of conducting an official review of documents, facilities, records, and any other resources that are deemed by the authority(ies) to be related to the clinical trial and that may be located at the site of the trial, at the sponsor's and/or contract research organizationís (CROís) facilities, or at other establishments deemed appropriate by the regulatory authority(ies).

Institution (medical)

Any public or private entity or agency or medical or dental facility where clinical trials are conducted.

Institutional Review Board (IRB)

An independent body constituted of medical, scientific, and non-scientific members, whose responsibility is to ensure the protection of the rights, safety and well-being of human subjects involved in a trial by, among other things, reviewing, approving, and providing continuing review of trial protocol and amendments and of the methods and material to be used in obtaining and documenting informed consent of the trial subjects.

Interim Clinical Trial/Study Report

A report of intermediate results and their evaluation based on analyses performed during the course of a trial.

Investigational Product

A pharmaceutical form of an active ingredient or placebo being tested or used as a reference in a clinical trial, including a product with a marketing authorization when used or assembled (formulated or packaged) in a way different from the approved form, or when used for an unapproved indication, or when used to gain further information about an approved use.

Investigator

A person responsible for the conduct of the clinical trial at a trial site. If a trial is conducted by a team of individuals at a trial site, the investigator is the responsible leader of the team and may be called the principal investigator. See also Subinvestigator.

Investigator/Institution

An expression meaning "the investigator and/or institution, where required by the applicable regulatory requirements".

Investigator's Brochure

A compilation of the clinical and nonclinical data on the investigational product(s) which is relevant to the study of the investigational product(s) in human subjects.

Legally Acceptable Representative

An individual or juridical or other body authorized under applicable law to consent, on behalf of a prospective subject, to the subject's participation in the clinical trial.

Monitoring

The act of overseeing the progress of a clinical trial, and of ensuring that it is conducted, recorded, and reported in accordance with the protocol, Standard Operating Procedures (SOPs), Good Clinical Practice (GCP), and the applicable regulatory requirement(s).

Monitoring Report

A written report from the monitor to the sponsor after each site visit and/or other trial-related communication according to the sponsorís SOPs.

Multicentre Trial

A clinical trial conducted according to a single protocol but at more than one site, and therefore, carried out by more than one investigator.

Nonclinical Study

Biomedical studies not performed on human subjects.

Opinion (in relation to Independent Ethics Committee)

The judgement and/or the advice provided by an Independent Ethics Committee (IEC).

Protocol

A document that describes the objective(s), design, methodology, statistical considerations, and organization of a trial. The protocol usually also gives the background and rationale for the trial, but these could be provided in other protocol referenced documents. Throughout the ICH GCP Guideline the term protocol refers to protocol and protocol amendments.

Protocol Amendment

A written description of a change(s) to or formal clarification of a protocol.

Quality Assurance (QA)

All those planned and systematic actions that are established to ensure that the trial is performed and the data are generated, documented (recorded), and reported in compliance with Good Clinical Practice (GCP) and the applicable regulatory requirement(s).

Quality Control (QC)

The operational techniques and activities undertaken within the quality assurance system to verify that the requirements for quality of the trial-related activities have been fulfilled.

Randomization

The process of assigning trial subjects to treatment or control groups using an element of chance to determine the assignments in order to reduce bias.

Regulatory Authorities

Bodies having the power to regulate. In the ICH GCP guideline the expression Regulatory Authorities includes the authorities that review submitted clinical data and those that conduct inspections. These bodies are sometimes referred to as competent authorities.

Serious Adverse Event (SAE) or Serious Adverse Drug Reaction (Serious ADR)

Any untoward medical occurrence that at any dose:

- results in death,
- is life-threatening,
- requires inpatient hospitalization or prolongation of existing hospitalization,
- results in persistent or significant disability/incapacity, or
- is a congenital anomaly/birth defect

(see the ICH Guideline for Clinical Safety Data Management: Definitions and Standards for Expedited Reporting).

Source Data

All information in original records and certified copies of original records of clinical findings, observations, or other activities in a clinical trial necessary for the reconstruction and evaluation of the trial. Source data are contained in source documents (original records or certified copies).

Source Documents

Original documents, data, and records (e.g., hospital records, clinical and office charts, laboratory notes, memoranda, subjects' diaries or evaluation checklists, pharmacy dispensing records, recorded data from automated instruments, copies or transcriptions certified after verification as being accurate copies, microfiches, photographic negatives, microfilm or magnetic media, x-rays, subject files, and records kept at the pharmacy, at the laboratories and at medico-technical departments involved in the clinical trial).

Sponsor

An individual, company, institution, or organization which takes responsibility for the initiation, management, and/or financing of a clinical trial.

Sponsor-Investigator

An individual who both initiates and conducts, alone or with others, a clinical trial, and under whose immediate direction the investigational product is administered to, dispensed to, or used by a subject. The term does not include any person other than an individual (e.g., it does not include a corporation or an agency). The obligations of a sponsor-investigator include both those of a sponsor and those of an investigator.

Standard Operating Procedures (SOPs)

Detailed, written instructions to achieve uniformity of the performance of a specific function.

Subinvestigator

Any individual member of the clinical trial team designated and supervised by the investigator at a trial site to perform critical trial-related procedures and/or to make important trial-related decisions (e.g., associates, residents, research fellows). See also Investigator.

Subject/Trial Subject

An individual who participates in a clinical trial, either as a recipient of the investigational product(s) or as a control.

Subject Identification Code

A unique identifier assigned by the investigator to each trial subject to protect the subject's identity and used in lieu of the subject's name when the investigator reports adverse events and/or other trial related data.

Trial Site

The location(s) where trial-related activities are actually conducted.

Unexpected Adverse Drug Reaction

An adverse reaction, the nature or severity of which is not consistent with the applicable product information (e.g., Investigator's Brochure for an unapproved investigational product or package insert/summary of product characteristics for an approved product) (see the ICH Guideline for Clinical Safety Data Management: Definitions and Standards for Expedited Reporting).

Vulnerable Subjects

Individuals whose willingness to volunteer in a clinical trial may be unduly influenced by the expectation, whether justified or not, of benefits associated with participation, or of a retaliatory response from senior members of a hierarchy in case of refusal to participate. Examples are members of a group with a hierarchical structure, such as medical, pharmacy, dental, and nursing students, subordinate hospital and laboratory personnel, employees of the pharmaceutical industry, members of the armed forces, and persons kept in detention. Other vulnerable subjects include patients with incurable diseases, persons in nursing homes, unemployed or impoverished persons, patients in emergency situations, ethnic minority groups, homeless persons, nomads, refugees, minors, and those incapable of giving consent.

Well-being (of the trial subjects)

The physical and mental integrity of the subjects participating in a clinical trial.

Appendix 2 – Computer Systems Classification

The purpose of this document is to define a method for determining and documenting which computer systems require validation and why. It also identifies systems that do not require validation and provides the necessary rationale for why they do not.

A2.1 Scope

This document covers all computer systems used at the data centre.

A2.2 Responsibility

Data Manager	It is the responsibility of each data manager to ensure that all computers within their area have been classified. It is also the responsibility of the department manager to notify QA when a computer has been decommissioned.
QA	It is the responsibility of QA to maintain the classification list.
IT and SW Engineering	It is the responsibility of individuals within IT and Engineering group to check the classification list prior to making any changes to computer systems.

A2.3 Procedure

There are several methods by which classification can be accomplished. To be successful, the procedure should have three components:

- A process for classifying the computer. This process should include QA review.
- A workable process for communicating a system's classification to those responsible for maintenance. There are a wide variety of methods by which this can be accomplished, ranging from placing a sticker on every computer system to incorporate it into a maintenance management system.
- A process for determining if a computer is considered a "legacy system."

A2.3 Important Issues to Address

Computer systems are pervasive. Often they may be embedded in equipment, they are included in most laboratory instruments, and they are on almost all desks. It is vital to know which computer systems are considered GCP critical (and therefore require validation and change control) and which ones are not. The decision process and the rationale behind the decisions need to be captured.

One method used for classification employs a tiered approach, instead of classifying systems only as critical or noncritical:

A2.3.1 Primary

These systems can have a direct impact on patient data safety, efficacy, identity, quality and therefore require the maximum level of GCP testing and documentation.

A2.3.1 Secondary

These systems are serving a GCP function but do not directly affect data in any way that impacts on patient data safety, efficacy, identity, quality. These systems still require validation but validation testing can be held to a lower standard.

A2.3.1 Legacy

Some computer systems have been in use for a long time. Again, these systems still require validation, but it does not make sense to recreate all life cycle documents for these systems (e.g. SAS, MS Excel).

A2.3.1 Non-GCP Systems

These systems have no GCP impact. But the centre may decide to document and test these systems, but the formality and approvals can be reduced.

A2.3.1 Other Systems

Other important points about the classification process:

- Some systems can be exempted from this procedure or pre classified as non GCP based only on their functional description.
- The classification decision process and associated rationale must be documented.
- For purposes of change control, a list of systems and their classification should be maintained so that appropriate personnel (e.g., maintenance, system developers) can verify the system's classification prior to making changes.