Deliverable No. D6.2

Evaluation report of the usability of p-medicine tools within the ECRIN infrastructure

Grant Agreement No.:	270089
Deliverable No.:	D6.2
Deliverable Name:	Evaluation report of the usability of p-medicine tools within the ECRIN infrastructure
Contractual Submission Date:	01/02/2014
Actual Submission Date:	01/02/2014

Dissemination Level		
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)	X

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.:	D6.2
Document name:	Evaluation report of the usability of p-medicine tools within the ECRIN infrastructure
Nature (R, P, D, O)[1]	R
Dissemination Level (PU, PP, RE, CO)[2]	CO
Version:	1
Actual Submission Date:	01/02/2014
Editor: Institution: E-Mail:	Wolfgang Kuchinke UDUS wolfgang.kuchinke@med.uni-duesseldorf.de

ABSTRACT:

To be employed in personalised medicine clinical trials, p-medicine tools have to meet many requirements for usage in large, international GCP trials. The tools have also to be integrated into existing clinical trial processes of the international ECRIN community. Developers of p-medicine tools were surveyed to evaluate the usability of p-medicine tools using requirements for GCP compliance, quality management, sustainability / business plan and process conformance. Software maturity and gap analysis showed that considerable gaps exist and that the tools in the present state cannot be employed by ECRIN. Nonetheless, the results of the gap analysis provide information to create recommendations how to prepare tools already during development for being validated for compliance and to be used in a GCP regulated environment.

KEYWORD LIST: requirements, regulations, GCP, tools, quality management, agile development, data security, pseudonymization, system validation, evaluation, ECRIN

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
0.0	01.04.2013	Draft	Christian Krauth
0.1	26.08.2013	Draft	Christian Krauth
0.2	03.01.2014	Draft	Wolfgang Kuchinke
0.3	18.01.2014	Draft	Wolfgang Kuchinke, Christian Krauth, Töresin Karakoyun, Holger Stenzhorn, Hena Ramay, Simona Rossi
0.4	23.01.2014	Draft	Wolfgang Kuchinke, Christian Krauth, Töresin Karakoyun
0.8	24.01.2014	Final Draft	Wolfgang Kuchinke, Töresin Karakoyun
0.9	28.01.2014	For review	Wolfgang Kuchinke
1.0	30.01.2014	Final	Wolfgang Kuchinke

List of contributors:

- Wolfgang Kuchinke
- Christian Krauth
- Töresin Karakoyun
- Holger Stenzhorn
- Gabriele Weiler
- Hena Ramay
- Simona Rossi
- Ioannis Karatzanis
- Christian Ohmann

Acknowledgement:

The authors wish to thank Steve Canham (Canham Information Systems and ECRIN strategic partner) for his help in simplifying the GCP requirement list.

Table of Contents

1 Executive Summary

To run clinical trials, it is necessary to have a clinical research infrastructure including an IT infrastructure in place that will allow the planning and managing of clinical trials compliant with Good Clinical Practice (GCP) and other European regulations and national regulations. ECRIN (European Clinical Research Infrastructure Network) is the pan-European infrastructure for clinical trials being developed to provide high-quality services for multinational clinical research. A usability evaluation for the employment of p-medicine tools in ECRIN was performed by a developer survey that covered two general aspects: first, usability within the ECRIN infrastructure and its processes and second, usability in a regulated area under GCP requirements and with validated tools.

A software maturity analysis was done with the help of developer interviews that showed to what kind of state of maturity the tools have been developed (alpha, beta, candidate). The following survey using questionnaires for self-assessment by developers was used to assess to what degree requirements concerning GCP compliance, validation, quality management, testing, business sustainability and process compliance is being met. Whereas the GCP and quality requirements were derived from the rules and regulations for validation, the process compliance requirements are based on an assumed model of using tools in personalised medicine trials by ECRIN including biosample management and imaging. A gap analysis used these data to analyse the state of compliance of ObTiMA, Dr.Eye and Biosample Manager. In addition, a risk assessment of using tools in the p-medicine infrastructure was performed.

The results show that p-medicine tools are still in an incomplete phase of development, with no candidate available to be employed in ECRIN trials. Gaps were detected in the area of quality management during software development and in the lack of a robust business model for sustainability. ObTiMA, Dr.Eye and Biosample Manager have to implement several features (e.g. query management) to be fully usable for ECRIN trials. A considerable change in attitude, processes and necessary controls was detected between the stages of software development as a project and as software as a product that will be used by potential customers. A model was created to improve this transition by feedback of requirements, features and specifications that correspond to the future customer perspective to the developer groups to enable a “compliance-by-design” approach. In this way, p-medicine tools can be developed considering requirements for GCP, validation, legal and procedural aspects personalised medicine aspects already during the development without having to wait for a complete system validation. This approach may result in tools with a higher quality, with little necessity for change and error correction and an easier way of enabling GCP compliance. The step of assessment of the developer by the user of the tool as part of the system validation is anticipated. Finally, recommendations for the developer group were developed to aligned p-medicine management and business strategy with the needs for usability of ECRIN and other future customers.

2 Introduction

2.1 What has to be evaluated?

The p-medicine project develops a set of software applications and tools that integrate into a security framework and provide with a joint portal support for the conduct of clinical trials in personalised medicine. Within the scope of the interaction of p-medicine with research infrastructures, the usability of the developed tools for clinical trials in the ECRIN network shall be evaluated. At first it should be determined what has to be evaluated. Part of this evaluation will be the usability of tools for clinical trials in a regulated situation. The usability of the p-medicine tools for the user, the quality of the corresponding GUI is being determined in another working package. Here, it will be determined if p-medicine tools can be employed and used in an international infrastructure that is experienced in providing services for clinical trials, but not yet with personalised medicine. Thus, the usability evaluation has to cover several aspects of ECRIN requirements at once:

- The business model of p-medicine (can ECRIN afford to receive or purchase p-medicine tools)
- Process view of p-medicine tools (can p-medicine tools be integrated into the ECRIN clinical trials workflow)
- Legal and ethical compliance aspect (GCP) (can p-medicine deliver compliant tools to ECRIN)

Usability in a network infrastructure requires collaboration (business model) and clinical trials requirements (GCP, regulatory compliance).

Technology and service provision has become quite common for clinical trials with a pharma industry sponsor. CROs (Clinical Research Organisations) as well as EDC vendors offer services to support clinical trials. EDC vendors provide data management services for different business models, fee for each data item collected, for each user, for each patient recruited. Often reduced fees are available for the support of academic clinical trials. Technology and service provision is focused on the support of well-paying pharma industry and no ideal solution for academic research centres is available. Large costs are necessary for purchase and yearly maintenance. In addition, the market for clinical trials technology is volatile, and companies are fast disappearing from the market or are being bought up. In this situation, ECRIN is interested in employing a sustainable solution that can justify investments in validation, configuration and training.

2.2 Usability and quality of software products used for clinical trials

The topic of this deliverable is the evaluation of p-medicine tools within the ECRIN clinical trials infrastructure. According to the DoW[3], to conduct a clinical trial, it is necessary to have not only an IT infrastructure; but also a clinical research infrastructure that will assist in planning and managing of prospective clinical trials. This is especially necessary for clinical trials that are compliant with GCP criteria and European regulations. ECRIN (European Clinical Research Infrastructures Network) is the pan-European infrastructure for clinical trials being developed to provide such an infrastructure to support high-quality services to

[3] DoW: From data sharing and integration via VPH models to personalised medicine, Annex I - "Description of Work", 2011-05-12

multinational clinical research[4]. ECRIN collaborates with several other research infrastructures like BBMRI, EATRIS, EUDAT and projects like EHR4CR[5] and TRANSFoRm[6] that develop the use of electronic health records for the collection of patient data, biobank access and translational data sharing including interaction with genetic databases, primary care databases and medical imaging systems. The inclusion of new sources of patient data for clinical trials requires the enabling of their interoperability. In the p-medicine project the necessity for data sharing and interoperability reaches a new degree of complexity; clinical trials patient data together with biobank access, imaging, genetic data, simulation data and data from hospital information systems (HIS) has to be integrated[7]. In addition, p-medicine tools have to meet requirements and conform to regulations to be used in large, international clinical GCP trials. According to the DoW, p-medicine shall be integrated into existing systems used by the ECRIN community. Integration covers aspects like adopting a legal and ethical framework and approved concepts for data security and pseudonymization, requirement system validation and service sustainability. All these aspects have to be addressed in an evaluation of the usability of p-medicine tools within the ECRIN infrastructure.

On the other hand, the provision of tools and services to the ECRIN community must have an added value for p-medicine too. Here comes into play of a simplified dissemination of p-medicine products in the area beyond oncological research into play. Because the ECRIN community is a well-structured and experienced group of clinical trial experts, p-medicine tools may find an interested customer.

The usability of p-medicine tools in ECRIN consists of many aspects; the most important is the GCP compliance. p-medicine tools will be employed in a distributed clinical research infrastructure in a regulated area. As a research infrastructure, ECRIN already several categories of software are in use[8]: (1) software not limited or dedicated to research, that is standard software, such as e-mail clients, word processors, (2) generic research software, and (3) specific research software. The first category, that covers software not limited to research, includes software like offices tools, e-mail clients, and operating systems. Generic research software supports general research processes offering general functionalities for research processes, without a focus on a specific research project. The third category, specific research software, covers specific solutions and is usually only used for a specific project. In clinical trials with p-medicine tools all three categories will be involved. In analogy to the tree categories, the data management system consists of two types, a generic type and a study specific type. A generic Clinical Data Management Systems (CDMS)[9] is configured for each trial. The Clinical Data Management Application (CDMA) is specifically configured for a single clinical trial (e.g. by employing a study specific eCRF). This characterisation will also apply to p-medicine tools. The data management component ObTiMA, but also the imaging and biobanking modules will have to be configured for every clinical trial anew. Usability of a software solution must cover these aspects.

[4] Demotes-Mainard J, Kubiak C: A European perspective – the European clinical research infrastructures network. Ann Oncol 22 (Suppl 7), vii44-vii49 (2011)

[5] EHR4CR: http://www.ehr4cr.eu

[6] TRANFoRm: http://transformproject.eu/Home_files/TRANSFoRm%20Project%20Summary.pdf

[7] Rossi S, Christ-Neumann ML, Rüping S, Buffa FM, Wegener D, McVie G, et.al.: p-medicine: from data sharing and integration via VPH models to personalized medicine. Ecancermedicalscience. 2011; 5: 218.

[8] Harms P, Grabowski J: Usability of Generic Software in e-Research Infrastructures. Journal of the Chicago Colloquium on Digital Humanities and Computer Science. Volume 1 Number 3 (2011)

[9] Ohmann C, Kuchinke W, Canham S, Lauritsen J, Salas N, et.al.: Standard requirements for GCP-compliant data management in multinational clinical trials . Trials 2011, 12:85 -105

Usability is a quality characteristic of the software[10] that has considerably influence on the handling of, and the user's attitude towards a software product. The ISO/IEC 9126 (1991)[11] defines six main quality characteristics: functionality, reliability, usability, efficiency, maintainability, portability and finally usability. Usability exists with regard to functionality and refers to the ease of use for given software. Also the ability to configure and learn how to use a system must be considered as major characteristics of usability. Usability affects economic aspects of software development and software deployment. In this context, usability can be seen as context-sensitive and this aspect has to be considered in our evaluation. Software that provides good usability in one application context can have little usability in a different application context[12]. To consider context sensitivity when evaluating the usability of p-medicine tools in ECRIN, as many as possible ECRIN network requirements should be considered which can represent the ECRIN clinical trials environment. The application context includes processes and tasks to be supported by the software, the environment in which the software is used (ECRIN clinical trial units network), and the users that fulfil tasks with the software (investigators at clinical trial units), the software maintenance and business requirements. The tasks to be executed with the software are user-oriented. One aspect to be considered is that increasingly data management services use cloud computing to support clinical trials. Cloud computing covers a set of infrastructure provisions through storage services, platforms, and applications. Software-as-a-Service (SaaS) has so far been quite successful with the provision of electronic data capture (EDC) services by large clinical trials data management system vendors. Clouds are characterised by an on-demand deployment model for virtual, flexible, highly scalable resources usually with a pay per use charge. Thus, it must be evaluated to what degree a cloud infrastructure and cloud based data storage may be a relevant business model for p-medicine.

Software employed in clinical trials must be of high quality. As a useful extension of software quality, the concept of "quality in use" has been defined[13] covering the degree to which a product used a specified user group can meet the needs to achieve specified goals with effectiveness, productivity and satisfaction[14]. The benefit for this concept is that it moves the focus of quality from the software as an isolated product to the user's needs, the processes supported and the context in which the software is used. Quality in use has several characteristics and sub-aspects that are important for clinical trials conduct:

- Effectiveness (accuracy and completeness of process support)[15]
- Efficiency (resources expended to achieve the user's goal)
- Satisfaction (degree in which the user needs are satisfied when the tool is used
    - Usefulness (perceived achievement of pragmatic goal by user)
    - Trust (confidence that the tool will behave as intended)
- Freedom from risk (degree to which a product or system mitigates the potential risk)

[10] Schweibenz W, Thissen F: Qualität im Web: benutzerfreundliche Webseiten durch Usability Evaluation (Berlin: Springer, 2003): 12.

[11] ISO/IECFDIS9126-1 Information Technology – Software product quality. ISO Geneva, Swiss

[12] ISO, Ergonomische Anforderungen für Bürotätigkeiten mit Bildschirmgeräten: Teil 11: Anforderungen an die Gebrauchstauglichkeit – Leitsätze (Brüssel: Beuth, 1999): 5.

[13] Bevan N.: Quality in use: incorporating human factors into the software engineering lifecycle. Software Engineering Standards Symposium and Forum, Proceedings of: Emerging International Standards. ISESS 97., Third IEEE International 1 Jun - 06 Jun 1997, Walnut Creek, 169 – 179 (1997).

See also: ISO/IEC 9126 Quality in use metrics

[14] Bevan N: Measuring usability as quality of use. Journal of Software Quality, 4, 115-130 (1995)

[15] In use qualities from ISO/IEC 25010. IRIT - UMR 5505. Online: http://www.irit.fr/recherches/ICS/projects/twintide/upload/435.pdf

  - Economic risk mitigation (degree to which the tool mitigates potential risks to financial status, efficient operation, commercial property)
  - Health and safety risk mitigation (degree to which the tool mitigates potential risks to patients/study subjects in the intended contexts (clinical trials)
  - Environmental risk mitigation
- Context coverage
  - Context completeness (degree to which the tool can be used with effectiveness, efficiency, freedom from risk in the specified context of use)
  - Flexibility (degree to which the tool can be used with effectiveness, efficiency, freedom from risk in contexts beyond those initially specified)

One possibility to include this aspect is to include target values for "quality of use" in the software requirements specification. In this sense, the evaluation of usability of p-medicine tools should consider the entire infrastructure of ECRIN and the use by a very heterogenic group of users.

There are several methods for evaluating the usability of software; often only a subset of measures is considered by employing one specific method.[16]. In p-medicine the evaluation of the usability of p-medicine tools plays an important role, an iterative evaluation process consisting of usability evaluation sessions and discussions has been established for this purpose. This process creates feedback reports, suggests possible improvements, modifications, and enables for the user a continuous learning process.

2.3 ECRIN clinical trials

As described above, a comprehensive evaluation of the usability of p-medicine tools must consider the context of use, in our case the employment of tools in the ECRIN network for large international clinical trials. ECRIN (European Clinical Research Infrastructures Network)[17] is a clinical research infrastructure consisting of a spike like structure representing the different national clinical trials networks. ECRIN is designed to bridge the fragmentation of clinical research in Europe through the interconnection of national networks of clinical research centres (CRC) and clinical trial units (CTU)[18]. ECRIN provides services to support multicentre clinical studies in Europe; currently 23 trials are supported. ECRIN is committed to support GCP (Good Clinical Practice)[19] in clinical trials and to support transparency. There is a need not only for commercial trials, but also for academic clinical trials to guaranty that the clinical trial is compliant to legal and ethical requirements and respects the international guidelines of Good Clinical Practice (GCP)[20]. This includes the commitment to employ in ECRIN GCP compliant data management systems to support the data collection in clinical trials. In a first FP6-funded step lasting 2004-2005, the status of clinical research in Europe was assessed in each country participating in the ECRIN project, and a comparative analysis between the countries was performed. The analysis demonstrated a considerable diversity between countries.

[16] Harms et.al.: Usability Idem

[17] Demotes-Mainard J, Ohmann C, Gluud G, Chêne G, Fabris N, et.al.: European Clinical Research Infrastructures Network Meeting Report. Towards an Integration of Clinical Research Infrastructures in Europe. Int J Pharm Med 2005; 19 (1): 43-45

[18] http://www.ecrin.org/

[19] ICH Topic E 6 (R1) Guideline for Good Clinical Practice, CPMP/ICH/135/95, EMEA London, 1996/2002

[20] A standard by which clinical trials are designed, implemented and reported so that there is public assurance that the data are credible, and that the rights, integrity and confidentiality of subjects are protected (Gerhard Nahler: Dictionary of Pharmaceutical Medicine. Springer Wien, New York, 2009)

An ECRIN wide survey determined the types of Clinical Data Management Systems (CDMS) in use, the resources available to the data management units and aspects of quality management and GCP compliance. It showed that about 90% of ECRIN centres have a CDMS in routine use[21]. The used CDMS were to nearly 50% commercial systems; Open Source solutions played only a minor role with seven different Open Source solutions identified. In addition, about 18 proprietary systems are in use. The most widely employed CDMS products were MACRO™ and Capture System™, followed by solutions that are used in at least three centres: eResearch Network™, CleanWeb™, GCP Base™ and SAS™. Although quality systems for data management are in place in most centres, there exist some deficits of proofs of complete and independent computer system validations.

ECRIN centres are very heterogeneous; most centres (31%) conduct less than 10 ongoing trials and employ less than 10 persons (30%); 19% of centres conduct 10-19 trials simultaneously. There exist some large centres that conduct more than 50 trials and employ more than 50 persons. Thus, ECRIN spans a wide range of different sizes of centres/units with a focus on smaller ones. An independent, external audit has been performed in 26 centres (41%); 82% of centres declared themselves able to provide an infrastructure and necessary human resources to support multinational clinical trials.

To address the issue of a high quality and GCP compliance in international clinical trials for clinical data management, ECRIN has begun to establish certified data centres. These ECRIN data centres support electronic data capture (EDC) and are able to handle the associated compliance needs of clinical trial centres in Europe. In 2011 ECRIN published a list of standard requirements for data management and IT infrastructure in trial sites[22]. This standard was developed by the Working Party 10 of ECRIN-PPI project. The standard is divided into two parts: an IT part covering standards for the underlying IT infrastructure and computer systems in general, and a data management part covering requirements for data management applications in clinical trials. The purpose of the standard is two-fold, to provide the basis of an ECRIN certification programme, i.e. applicants audited against the standards to confirm their ability to provide compliant and effective data management services, and for ECRIN supported trials to provide a clear interpretation of regulatory and good practice requirements. The standard provides GCP requirements in the context of the limited resources available at non-commercial trials units in Europe. Thus the standard can be used as a general guide to establish and manage high quality data management services. In 2012, after two pilot audits, the ECRIN standard has been revised and enriched with interpreting documentation. The question arises if the ECRIN standard can cover the extended requirements for GCP compliance that are associated with the IT infrastructure used in personalised medicine trials? Because ECRIN data centres will support European international clinical trials, the considerable heterogeneity of CDMS may be a hindrance for international cooperation and trial data exchange and to conduct trials in personalised medicine.

2.4 GCP compliant clinical trials and service provision

WP 6 of p-medicine deals with the integration of p-medicine tools and services in the existing clinical research infrastructure ECRIN. One necessary step in the integration of tools is the evaluation of the usability of p-medicine tools/services in order to assess the potential benefit / usability of these tools for the ECRIN community. One of the preconditions for p-medicine

[21] Kuchinke W, Ohmann C, Yang Q, Salas N, Lauritsen J, et.al. Heterogeneity prevails: the state of clinical trial data management in Europe - results of a survey of ECRIN centres. Trials. 2010 Jul 21;11(1):79-89

[22] Ohmann C, Kuchinke W, Canham S, Lauritsen J, Salas N, et.al.: Standard requirements for GCP-compliant data management in multinational clinical trials. Trials 2011, 12:85

tools is that they have to be validated for GCP compliance. This validation step is necessary to demonstrate that a system has been developed and implemented, and is operated and maintained, in a controlled manner. The result of such a validation is a high degree of assurance that the system consistently meets its specification and is suitable for its intended purpose[23]. The validation process is called Computer System Validation (CSV), a technique that companies and institutions use to ensure that each IT application fulfils its intended purpose. Quality requirements in GCP compliant clinical trials impose needs for controls and procedures throughout the entire Software Development Life Cycle (SDLC). Evidence that these controls and procedures have been followed has to be created and must be produced in the case of audits. It must be documented that controls and procedures resulted in quality software, software that satisfies its specified requirements, does not endanger the patient and doesn't compromise or corrupt data in clinical trials. The CSV requirement is tightly coupled to the quality of the software product and is another aspect of the usability of a software solution for the ECRIN community.

It is to be expected that ECRIN will conduct personalised medicine trials in future. But to cope with the increasing demands for data centres caused by the high volume of digital information and their heterogeneity of data in personalised medicine trials and exchanged across different centres, it is inevitable that ECRIN data centres have to provide reliable and trustworthy data management services. GCP demands not only to have measures in place to protect the safety of clinical trials participants but also the quality of clinical trials data. But the "GCP compliant data management" has to be clarified in the context of multinational multicentre clinical trials and issues of trust in the authenticity of data management processes, data security and the associated issue of quality assurance must be treated as overarching priorities in ECRIN.

For an evaluation of usability in ECRIN, it must be considered that many ECRIN centres have their own CDMS in use. Any integration of new tools has to show an added value for ECRIN, to make clinical trials conduct easier, faster and more efficient. ECRIN demands that any new tool to be employed in ECRIN should be usable for all types of clinical trials, not only for cancer trials, and not only for personalised medicine trials. Preferable biobank access and safety functions should be integrated with the CDMS to provide easy access and query functions to existing biobanks. In addition, maintenance, support and updates should be available and the tool should afortable for academic researchers. The integration of data from multiple sources (laboratory data, molecular biology data, genomic data, images, EHR) should be supported and standards (e.g. CDISC) should be used. p-medicine tools will provide ECRIN with necessary tools to conduct clinical trials with imaging and biobanking access, but also clinical trials in personalised medicine.

p-medicine may offer data management services to the ECRIN community. These services must be integrated into the available infrastructure of ECRIN that itself provides clinical trials services for the trial sponsor. Service integration may involve Software-as-a-Service (SaaS) such as data management services, clinical data query services, patient empowerment service; in contrast Platform-as-a-Service (PaaS) provides tools to develop own applications such as databases, operating systems, etc.; Infrastructure-as-a-Service (IaaS) enables access to computer infrastructures such as servers, data centers and network equipment (security infrastructure, pseudonymisation/anonymisation tool). In principle, p-medicine may provide not only a software product, but any of these service types. Two possibilities exist for ECRIN: tools will be partly installed and run at an ECRIN data centre, or partly services will be provided by p-medicine or a third party (e.g. Trusted Third Party services, Custodix). The use of services instead of the purchase of a new software tool should be easier to accomplish for ECRIN and other customers.

[23] Stokes T.: Validation of GCP Systems at Investigator Sites. ACT Feb. 1997, 46-50

The service based approach results in several concerns and challenges. One of the major concerns of cloud based service providing for the health industry is compliancy. Pharmaceutical companies must ensure that cloud service providers follow GCP requirements as outlined by the Annex 11 (21CFR-Part11) regulation; including the necessity for IP/IQ (Installation protocol and installation qualification), OQ (Operational qualification) and PQ (Performance Qualification). System validation of a clinical cloud application means that the user as service consumer cannot have an installation protocol for installation of the hardware, because installation is done at the location of the service provider, whereever this may be. A test and production environment for each application in the cloud must be provided. Testing data backup and restore of all production applications must be ensured. Validation of software applications must take place in the cloud and the same validation documentation must be created as if the application is running on a local server. Since clinical trials are more and more international, there is also a need to ensure that local regulations are followed and it may, for example become necessary to know where the clinical trials data is hosted. Indeed some countries require the clinical data only be hosted in the actual country of the clinical trial. In addition, a service provider for clinical trials has to employ a service strategy, including documented processes for service design (service level, availability, security, requirements, continuity, and change), service operation (incident, access, service desk) and quality management. In addition service validation and usability testing have to be done. This will be challenging for many academic service providers and thus also for p-medicine.

2.5 Computer system validation (CSV)

The purpose of CSV is to provide an organized and consistent plan to ensure the integrity and quality of a computerized system throughout the life cycle of a system. It is best practice to develop and maintain standards and procedures such that all computer systems in use in a regulated environment be implemented and maintained in a validated state. Typically, policies/controlled documents are created to ensure the validation of computer systems used to generate, manipulate, store or transmit data related to all regulated products or services. In general the validation process follows a modified V-model for validation[24]. The V-model is a Software Development Life Cycle (SDLC) aspect that shows how three qualification activities (installation, operation and performance) are linked back to design processes. These main activities correspond to documents within the computerized validation framework. The left side of the V represents the specification stream (user requirements, functional specifications, hardware and software design, and module specifications) and the right side represents the verification stream, the testing against the specifications. The document that initiates the validation process is called user requirement specification (URS). The URS describes the system as it is intended to function, and it is typically written by the system user. A clear documentation of a properly functioning system as detailed in the URS defines what the system should do and what it could do. The process proceeds from documentation and Code Review, to iterative system specification, configuration and development of a IQ/OQ Protocol (Installation Qualification and Operational Qualification), corresponding test scripts and a validation result report. Often the Functional Requirements are defined in a User Acceptance Protocol and corresponding test scripts. In general the CSV generates following steps and documents:

- Computer System Validation
- Purpose of Computer System Validation
- Master Validation Plan
- User and Functional Requirements Specification

[24] GAMP4

- System Specification and Configuration Document
- Test Plan, Test Scripts and Test Summary
- IQ/OQ Protocol, Test Scripts and Summary Report
- User Acceptance Protocol
- Validation Summary Report
- System Maintenance
- System Retirement

A Master Validation Plan (MVP) should describe the activities, procedures and responsibilities associated with validating the system. The document should describe the approach that will be taken to assure that the system has been developed according to quality software engineering principles and the approach to ensure that regulatory requirements are addressed during the implementation and the operation of the system.

In the context of system validation, the provision of clinical trials software as service has an considerable impact on the way to validate the system. For example, more and more services are offered in a cloud, including services that support clinical trials. But to run a clinical trial clinical trial quality, compliance, validation, security and legal compliance are major hurdles. Assessing and mitigating the risks of hosting GCP regulated applications in the cloud may be one way to reduce efforts and costs. The main risks running a service based clinical trials application are: data/information security (use of VPN and encryption), platform and application architecture (e.g. multi-tenancy), ignorance of service providers to understand the processes of personalised medicine and the issues of regulatory requirements (GCP compliance). Because service providers are focused on their business needs, the user has to decide between different levels of security (private vs. public clouds, anonymization vs. pseudonymisation). A lot of privacy and security problems arises from cloud computing, which may be critical for clinical trials. In addition, the problem of business continuity of services (e.g. internet access at the investigator site) has to be dealt with. During a clinical trial, that may last several years, it may not be possible to change service provider. But in case of service provider change, data migration problems, new security validation, ensuring the necessary performance level (e.g. bandwidth) at client side have to be considered. Particularly, patient privacy must be protected, and it may be necessary to audit the investigator site where patient data is being kept. Each investigator must be in control of the own source data, which must be stored separately from the clinical trials data[25]. In general source data is EHR data (if not electronic source) and the investigator has to keep control over his eCRF/paper CRFs. Especially three GCP requirements deal with this responsibility[26]:

- An instrument used to capture source data should ensure that the data are captured as specified within the protocol (this concerns the EDC system and the eCRF)
- Source data should only be modified with the knowledge or approval of the investigator
- The sponsor should **not** have exclusive control of a source document (this implies that the investigator must have this control).

The user should consider that there is a difference in qualification of a cloud-based environment versus the validation of an application in a regulatory framework[27]. In general, the application should be validated and the IT infrastructure should be qualified regardless if the application is hosted at p-medicine or in an ECRIN data centre. Audit authorities and

[25] EMA: Reflection paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials. EMA/INS/GCP/454280/2010, London (2010)

[26] EMA: Reflection paper on expectations for electronic source data, idem

[27] Hulleman R: Application validation versus infrastructure qualification. ISBT Science Series 8, 70–72 (2013)

GCP/GMP regulations (e.g. Annex 11 and GAMP) require a qualified infrastructure. To qualify an infrastructure, it is useful to split it into testable modules. Because p-medicine is built in a modular way, a modular validation may be easy to achieve. The process of building these components has to follow quality requirements (Annex 11). The typical qualification documents include specifications, IQ documentation scripts, plans and reports, agreements with service providers, operational procedures. The infrastructure qualification documents are also needed when a regulated and already validated application is hosted in a cloud environment, because the need for a validation of the application does not change, wherever the application may be installed. A suitable qualification and validation strategy may help to mitigate the risks associated with using a service provider, and generate auditable evidence to show how this has been done by considering for example the VM-level security, a multi-layered defence, patch management, data protection and encryption.

2.6 Quality management in software development

From the QA perspective, the validation of applications or cloud based service solutions GCP compliant applications need to be completely validated, requiring in one case a developer audit and in the other case a service provider audit. In addition, in case data privacy needs exist, data privacy requirements should be tested as part of the validation. Enhanced validation processes should ensure that risk is managed. The more the service providers understand GCP requirements the easier their infrastructure can be qualified for production uses. For example, SaaS examples exist where pharma companies are using private cloud arrangements for their software applications.

According to GAMP, software and computer systems should be validated and qualified during the entire duration of the software life cycle[28]. When software or computerised systems are purchased from a vendor/producer an important question raised is who is responsible for the validation of the system: the vendor or the user? GAMP, but also the OECD consensus paper 5 states that it is the responsibility of the user to ensure that the software is validated. However, the quality of the software cannot be achieved by testing at the user site. Quality must be incorporated during design and development, which can only be done by the provider. It may be acceptable for formal validation to be carried out by the supplier on behalf of the user. Furman of the FDA also says that manufacturers should have validated their software before releasing it. A recent OECD consensus paper requires the development of software in a quality system environment. Similarly Annex 11 requires that the user shall ensure that software has been produced in accordance with a system of quality assurance.

For software development this usually means that the software is developed and validated following documented procedures. The user should ensure that the software has been validated during development even if the user has no insight into the vendor's practice and often doesn't has the technical understanding of how software should be validated during development. There should be a software vendor qualification scheme that certifies software vendors to be compliant with all regulations and with GCP. Even though such software certifications exists (ITQS or TickIT), none is suitable for regulated software and not sufficient for a vendor qualification. Development of an efficient vendor qualification program,

According to GAMP5's description of software provider/developer activities[29]; the software provider should participate in the validation. The suitable role of the software developer/ provider during validation must play an important part in the usability evaluation. The

[28] Huber L.: Qualification and validation of software and computer systems in laboratories. Accred Qual Assur 3:2-5 (1998)

[29] GAMP5, ISPE 2008 idem

relationship between provider and user can vary according to the products and services delivered. GAMP knows several categories of products: non-configurable product (GAMP categories 3): no configuration is necessary to support business processes. Configurable products (GAMP categories 4) the assistance of the provider comprises support during specification, configuration, verification and the operation of the systems. This category applies to p-medicine tools, which are highly configurable to adjust the tools to the different specifications of various clinical trials. Custom specific applications (GAMP categories 5) require support during system operation that has to be ensured on a contractual basis.

2.7 The Software Development Life Cycle

The software development life cycle (SDLC)[30] describes a process of a series of steps which should ensure that the target software is properly developed in an organised and well-structured way. This sequence of steps for the development of a software tool plays an important role during development, risk analysis and testing. The process contains five main phases:

- Planning
- Analysis
- Design
- Implementation
- Maintenance

There are different general models to use these SDLC phases, e.g. waterfall model, V-Model (mentioned earlier) or agile development model. Every phase has its own processes and deliverables which are the base for the next phase.

Planning

Every SDLC starts with the planning phase. It is the base for all upcoming steps and important for the success of the project. The aim of this phase is to understand the stakeholder and user needs and the purpose of the software. To gather this information (requirements) techniques like interviews, surveys, analysis of documents, observations and workshops can be used.

Analysis

After gathering all requirements the analysis phase inspects the needs of the users in order to arrive a successful outcome of the requirements. The requirements analysis aims to deepen the understanding of the constraints and user needs.

Design

The design phase defines how the software will be written. This phase is also known as requirements specification and elaborates the requirements based on use cases and scenarios. It contains amongst others risk analysis, functional specifications and non-functional specifications.

Implementation

In the implementation phase the actual tool (code) for the project gets developed and implemented. Furthermore the implemented product gets tested and checked for errors, bugs and interoperability. The final stage of the implementation is the acceptance, installation and deployment process where the software gets into the live system and it actually gets used.

[30] Lewis J. SDLC 100 Success Secrets - Software Development Life Cycle (SDLC) 100 Most Asked Questions, SDLC Methodologies, Tools, Process and Business Models. Newstead: Emereo Publishing; 2008.

Validation and Evaluation

A sub phase of the implementation is validation and evaluation of the developed tool. The evaluation checks if all requirements, regulations and quality issues are met and if the tool was developed in a well-structured way. The validation handles with the migration of the developed tool into the running system of the user or customer. Hereby it is important to have a fall back strategy if the tool doesn't fit into the productive environment.

Maintenance

The last step of the SDLC is software maintenance. Hereby the main activity is to modify the product after delivery. Amongst others a modifying can be necessary to improve performance or to correct not discovered bugs.

3 Methodological approach

3.1 Methods for the assessment of tool maturity

3.1.1 Questionnaire development

The assessment of the maturity of the involved tools / services is necessary to have an overview about the actual status of the tools. With this information it is possible to classify the tools and create an evaluation strategy for the different states[31] (Appendix 7.2).
The questionnaire for assessing the maturity of the involved p-medicine tools (Appendix 7.2.3) is divided into the following nine sections:

- General information
- Software development process
- Organisation/ general aspects
- Continuous delivery
- Specification
- Software, tool or service provision
- Testing
- Quality management and support documents
- Licenses

The questions dealing with general information was not considered in the questionnaire and was used to get to know the developer group and to get an understanding of the structure of the tools. In the question about software development, developers gave their own judgements about the maturity of the software. This opinion was discussed with developers in light of the results of the questionnaire and if necessary corrected. The questions of this questionnaire were created based on two documents: "TMF Systemvalidierungsmasterplan (SVMP)"[32] and "Revising the ECRIN standard requirements for information technology and data management in clinical trials"[33] and adapted to the purpose of the survey.

3.1.2 Conduct of interviews and assessment

To get the maturity information the interviews were conducted directly (face to face with the developer), via telephone and via email. The respondent could answer with yes, no, not applicable.

The first contact with the developers took place in the "p-medicine usability workshop" in London at 24th and 25th July 2013. Here the questionnaire was explained and questions about it answered, furthermore the questionnaire was filled from the developers. Afterwards developers who weren't at the workshop were contacted via telephone and email and also helped to complete the questionnaire.

For the analysis of the survey results, selected chapter (criteria) got a coefficient to assess the given answers. The maximum reachable points of each chapter are six and get divided into the different answers. If requirements respectively questions are not completely fulfilled or are in a planning phase, only half of the points were given (Appendix 7.3).

[31] maturity status = current state of the development of the software

[32] http://www.tmf-ev.de/Produkte/Uebersicht/ctl/ArticleView/mid/807/articleId/280/P019011.aspx

[33] http://www.trialsjournal.com/content/14/1/97

3.2 Risk assessment

Independently from the maturity assessment, a risk assessments for the three main tools, which are already at an advance development stage, was conducted; Portal, Ontology Annotator (OA) and, ObTiMA. These tools were chosen as they are the main user interaction front ends of p-medicine and therefore of special importance for the usability of p-medicine. Risk assessment was conducted exemplarily for all tools and the other tools have to be assessed accordingly. A risk analysis template is attached (7.1.1.) Each tool's developers were requested to identify risks pertaining to their tool and its impact on p-medicine in general. For each risk, its probability and impact (on a tool itself and on p-medicine as a whole) were classified as low, medium or high. For each risk, a mitigation plan, contingency plan and a responsible person/team were also identified.

3.3 Requirements for compliant system use in ECRIN trials

3.3.1 The problem domain of which the questionnaires were developed

The requirements for our survey were received from the problem domain of data management for clinical trials, the area of the conduct of regulated clinical trials. This area is dominated by laws and regulations and their interpretation that is laid down in rules and guidelines. Because the interpretation of laws and regulations plays such an important role, the sources have to be discussed. All sources were used to obtain requirements and specifications for the questionnaires. Three kinds of questionnaires were developed assessing these requirements: (1) Quality management during the development process and GCP compliance, (2) Technical and compliance requirements for the conduct of personalised medicine trials in ECRIN (specifically for ObTiMA, biobanking and imaging (Dr.Eye) and (3) Business and sustainability requirements. For the evaluation of p-medicine tools to be employed by ECRIN for GCP clinical trials all three aspects are of importance. For software tools the GCP compliance implies that all tools are validated (CSV) before being employed. Especially, the relationship of CSV to the Software Development Life Cycle (SDLC)[34] is of importance because, CSV is influenced by activities that occur throughout the entire SDLC. The “V model” of CSV is a method used in IT to emphasize the importance of testing at every step in the SDLC. But the V-diagram can also be seen only as a transcription of the often criticized “Waterfall” model of SDLC. Thus the question arises: can it be efficiently used in agile computing?. The phases in the Waterfall model are essentially the life cycle phases that appear on the left-hand side of the V-diagram. The activities represented in the V-Diagram include Static Testing as well as Dynamic Testing activities. A three level structure is imposed on User Testing: Installation Qualification or IQ focuses on testing that the installation has been done correctly. The Operational Qualification or OQ focuses on testing of functionalities in the system installed at the User site and the Performance Qualification or PQ focuses on testing that users, administrators, and IT support people trained in the SOPs can accomplish their tasks in the production environment even under every day working conditions.
FDA requirements for computerised systems used in clinical trials[35] and other FDA guidelines were not considered, because p-medicine trials will be take place for the moment in Europe. The evaluation questionnaires list requirements for the evaluation of p-medicine tools for clinical trials usage in ECRIN trials. For the development of the questions/requirements following sources were consulted:

[34] Petschenik N: Computer System Validation - It’s More Than Just Testing . STS, 2007

[35] Guidance for Industry Computerized Systems Used in Clinical Investigations. Food and Drug Administration (FDA), May 2007

- GAMP® 5: A Risk-Based Approach to Compliant GXP Computerized Systems. ISPE Tampa, FL, USA
- EudraLex, The Rules Governing Medicinal Products in the European Union, Volume 4: Annex 11: Computerised Systems (2010)
- ICH Topic E 6-Guideline for Good Clinical Practice. EMEA 2002
- Standard requirements for GCP-compliant data management in multinational clinical trials. Trials. 2011; 12: 85
- IT-Grundschutz Catalogues (BSI), 2005
- ISO 27001
- ISO17025
- Software Development Review Checklist. ITS.
- BIOREQ-Model requirements for the management of biological repositories, version 2, ASTRIDBIO
- SOFTWARE QUALITY ASSURANCE CMM traceability checklist, University of Colorado, VAST
- ASQR 07.5: Control of Software (Checklist), United Technologies, 2008
- GENOMatch-University, validation report, Tembit 2013
- Catalogue of Requirements. Software Support of Clinical Studies (with emphasis on Remote Data Entry). For Software Producers and Providers. TMF, 2002
- Questionnaire for evaluation of EDC-Systems. KKS Network, 2012
- Best Practices for Repositories 2012 (Collection, Storage, Retrieval, and Distribution of Biological Materials for Research), ISBER 2011

GCP compliance regulations is an area that needs conciderable interpretation of the a rather somall number of regulations. For this reason several documents were used in more detail to establish of the requirements for the questionnaires:

The **GAMP Guide for Validation of Automated Systems**[36] is widely used and internationally accepted. GAMP Forum (Good Automated Manufacturing Processes Forum) that has developed the GAMP Guide focuses on the application of GXP requirements to the IT environment. GAMP requirements, especially for developer / user collaboration and business requirements were considered for our asessment questionnaires. In fact, the GAMP guide is a collection of requirements from many relevant guidelines (like PIC/S, Annex11, etc.) but leaves place for interpretations of requirements.

An additional document to consider is the **Aide-Mémoire** (AiM) that in the first part contains a short introduction for the inspection of computerized systems. The second part covers explanations of the EU GMP Annex 11 requirements and commented questions often addressed during an inspection. According to the AiM, the basis for the operation of a computerized system in any GXP area should be a documented risk assessment based on pre-defined, justified and traceable criteria[37]. This risk assessment should consist of methods and approaches which analyze computerized systems to a sufficient level of detail regarding outcomes and impacts to the pharmaceutical product, patient safety, quality of data sets and data integrity. The outcome of this risk assessment is the basis for the decisions about the scope of validation and this requirement has to be considered for questionnaire development. In our approach this relationship is represented by the analysis and evaluation of the quality management during system development.

According to the AiM the software developer evaluation plays an important role, especially when software suppliers and service providers are involved. When third parties (e.g. suppliers, service providers) are used to provide, install, integrate, validate, maintain, and modify a computerised system and related service for data processing, formal agreements

[36]GAMP 4 and GAMP5, idem

[37]Aide-mémoire 07121202: Inspections of computerized systems, ZLG, German ZLG (Central Authority of the Laender for Health Protection)

must exist between the manufacturer/software provider and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT departments should be considered in an analogous way as service providers. The supplier evaluation, the functional specification and further qualification documents should be in place, and audit reports should exist for review (to provide an insight into the audit processes). If it is the case that process of software development is executed by a third party and cannot be under full control by the user, the supplier evaluation and assessment has a extraordinary relevance to verify that the software is developed according quality assurance methods.

PIC/S guidance[38] sets similar requirements for "GXP" inspectors and it provides recommendations and information concerning computerised systems that will be of assistance to inspectors for training and during the inspection process in the regulated pharmaceutical area. It states that commercial 'off the shelf', 'standard', or proprietary systems can be particularly difficult to assess from a quality and performance point of view. For GxP regulated applications it is essential for the regulated user to define requirement specifications prior to the selection of the application and to carry out a properly documented supplier assessment and risk analysis for the various system options. Information for the supplier assessment may come from supplier audits and research into the supplier's product versions in the user community and literature. This risk-based approach is one way for the software developer to demonstrate that a controlled methodology was applied, and to determine the degree of assurance that a computerised system is fit for purpose.

The degree of reliability of a software product is in general attributable to the quality of the entire software engineering processes followed during the development process. This should include design, coding, verification testing, integration, and change control features of the software development life cycle, (including support and maintenance). In order for the user to have confidence in the reliability of the product, they should evaluate the quality methodology of the software supplier for the design, construction, supply and maintenance of the software. A formal review of the history of the supplier and the software package may be an option to consider where an additional degree of assurance of the reliability of the software is needed. This should be documented in a "Supplier Audit Report". Prospective purchasers should consider any known limitations and problems for particular software packages or versions and the adequacy of any corrective actions by the Supplier. In addition a comprehensive and documented customer acceptance test should support the final selection of the software package. Because errors often emerge only after the implementation step, it is important for the software supplier to advise/assist the customer with any problems and modifications to resolve errors.

The guide stresses, that unfortunately a high level of assurance of quality and reliability cannot be attributed to a computerised system based simply on a series of tests solely designed to confirm the correct function of the software and its interaction with hardware. Thus, a formal planned approach by the software developer to assure that quality is built into the product is needed. For example, ISO 9001 provides a quality system model for quality assurance in design, development, production, installation and servicing. The objective of this testing approach during software development is that the software supplier should break the structural integrity of the software and find any weaknesses through a rigorous testing regime. Audits of suppliers conducted by or on behalf of regulated users should cover these issues when project related risk analyses deem it to be necessary. In this way, it is important for a regulated user to have in place a comprehensive policy and procedures for the specification, purchase, development and implementation of a computerised system. Ideally

[38] Pharmaceutical Inspection Co-Operation Scheme : Good Practices for Computerised Systems in Regulated "GXP" Environments, PI 011-3 , 25 September 2007

these procedures would cover all computerised systems in place in a data centre; but PIC/S guidance concerns itself only with systems that have an impact on GxP.
It is important to acknowledge that the scope and level of documentation and records needs for critical systems depends upon the complexity of the system and variables relating to quality and performance; the need to ensure data integrity; the level of risk associated with its operation; and the GxP impact involved. Compliance with the GXP standard requires formal systems for control, traceability and accountability of the product and personnel. The standard outlines the features and requirements of a life cycle approach to software production with emphasis on the importance of change control. The need for, and importance of, testing of software product/s tiered approach to testing and identifies three levels of testing for software Unit code testing; Integrated module testing; and Customer acceptance testing. Regarding quality assessment during software development, one of the most critical aspects is the integration testing phase where individual elements/modules of software code are combined and tested until the entire system has been integrated. Because p-medicne is constructed from modules, integration testing is expected to play an important role and a validation of this process might be useful.
Extra benefits may be achieved by code walkthroughs including evaluation of critical algorithms and routines, prior to the test step. Test scripts should be developed, formally documented and used to demonstrate that the system has been installed, and is operating and performing satisfactorily. These test scripts should be related to the User Requirements Specifications and the Functional specifications for the system. This schedule of testing should be specifically aimed at demonstrating the validation of the system The supplier/software developer should draft test scripts according to a project quality plan to verify performance to the functional specifications. In addition, the scripts should use stress test to check for structural integrity, critical algorithms and “boundary value” aspects of the integrated software. However, this may be difficult to apply to complex integrated computerised systems where different GAMP category “levels” are effectively combined. Inspectors are interested in the software supplier's approach to identifying GXP risks and the criteria for assessing the fitness for purpose of the system application.
The key aspects of the security of infrastructure, system and specific application to be controlled and managed are:

- existence of an authorised user log-on for the application
- a unique combination of user ID and password linked to the user’s authorised account
- definition of a permitted task functionality for the user
- defined time zone and date standard referencing
- relative transaction linking (e.g. for spanning several time zones)
- audit trail
- physical and logical system security with control features
- Issues to consider where electronic records are used to retain GXP data:
- documented evidence of compliance
- archiving procedures
- procedures exist to ensure accuracy, reliability and consistency in accordance with the validation of the electronic record
- system controls and detection measures exist to enable the identification, quarantining and reporting of invalid or altered records
- procedures exist to enable the retrieval of records throughout the retention period
- ability to generate accurate and complete copies of records in both human readable and electronic form
- access to records is limited to authorised individuals only
- secure, computer-generated, time-stamped audit trails to independently record GXP related actions

Annex 11[39] is concerned with the use of electronic records that result in additional requirements for the regulated software. It corresponds to the European version of 21CFR Part11[40]. According to Annex 11, risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. Decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.
For software suppliers and service providers Annex 11 demands that in case third parties (e.g. suppliers, service providers) are used to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous. These requirements are part of the business questionnaire, but will depend on the business model of p-medicine.
The competence and reliability of a supplier are key factors when selecting a product or service provider. Therefore, the need for an audit should be based on a risk assessment. It is of importance, that physical and logical controls should be in place to restrict any access to the computerised system to authorised persons only. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.
Business Continuity must be demonstrated; for the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown. This may include a manual or provision of an alternative system. The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.

3.3.2 Structure of the survey

Based on the requirements that have to be considered when running a GCP compliant trial (GCP, PIC/S, regulations, QA/QM,…) two kind of questionnaires were developed (Fig. 1). First, generic requirements cover the business model and the sustainability aspects as well as quality management/ develoment management of the developer groups. These are all important aspects of a potential developer assessment by a tool user (ECRIN). Second, tool specific requirements were generated from a model of a clinical trial run by ECRIN including in addition to data management, the processes for imaging and biobanking. These requirements are more technical in nature and contain specifications for the developer that are to a large degree not mandatory, but a suggestion that may be met by different technical solutions (e.g. pseudonymisation of biosamples with bar codes, or other devices). Results of both questionnaires were used for a gap analysis to assess what requirements and to which degree are met.
On the basis of the results of the generic requirements questionnaires, criteria were extracted to generate recommendations to improve quality aware software development. It is the aim to incorporate as many compliance requirements, required documents and needed checks as possible into the development process. In this way a later developer assessment by the user becomes much easier, both for the user (purchaser) and the developer groups (tool vendor).

[39] EudraLex : Volume 4 GMP. Annex 11: Computerised Systems , 2011
[40] http://www.fda.gov/regulatoryinformation/guidances/ucm125067.htm

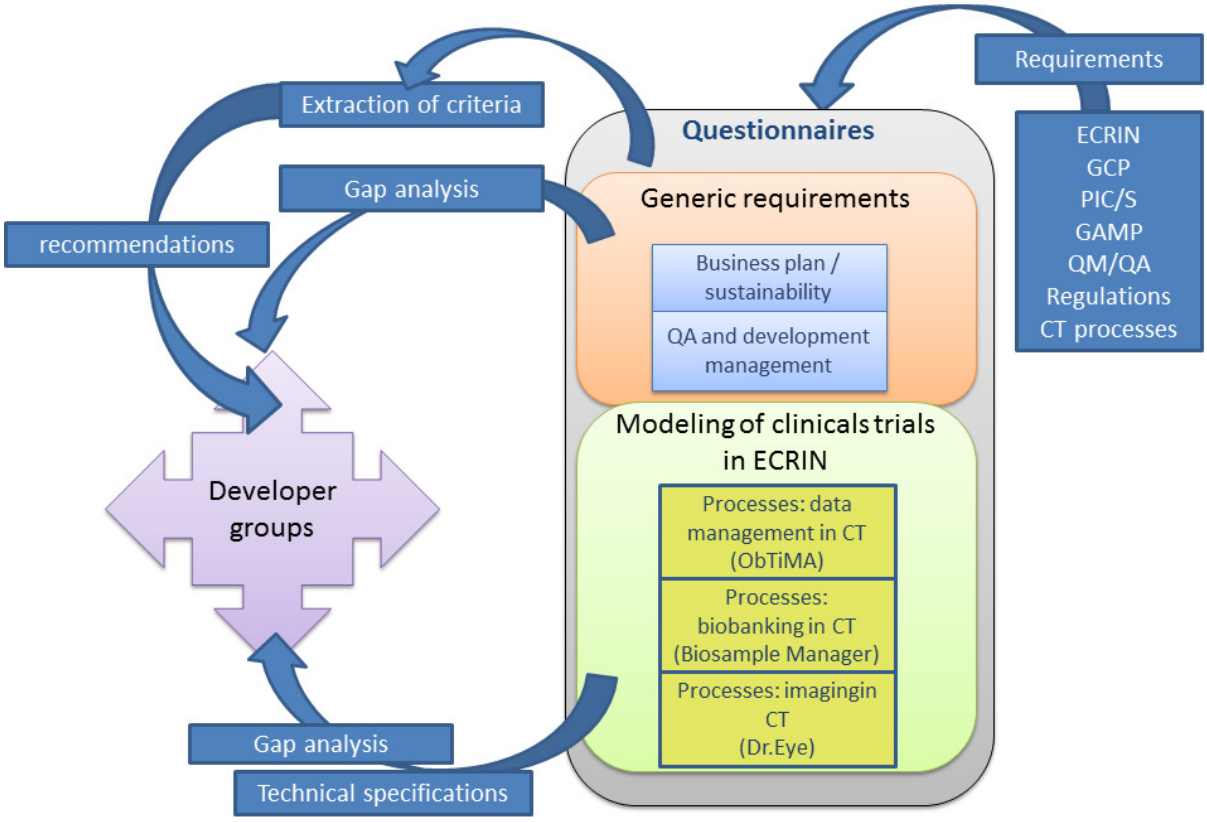


Fig.1: Structure of the survey and dependencies of the results of the gap analysis, the technical specifications for conducting clinical trials and the developed recommendations.

3.4 Composition of the Questionnaires

Based on a number of guidance documents, a number of relevant requirements were created. The main requirements are listed according to their inclusion in the different evaluation questionnaires:

3.4.1 Questionnaire for the p-medicine business model

The sustainability of the provided tool / services is of utmost importance for the tool user. Clinical trials can last several years and the use of the a tool results in the need for maintaining and training that requires considerable resources for the trial sponsor. First, the composition of the developer group has to be examined:

- Number of developers, number of supporting staff members?
- Are the responsibilities of each member in the group described?
- What are the experiences of the member of the developer group?
- Prior projects in the field of medical research?
- Is an organogram of the software development group available and current?
- Does the development group have sufficient qualified and experienced personnel in order to adequately perform the development of p-medicine software tools?
- The ability to participate in a vendor / developer assessment should be proved.
- Permission for developer/vendor assessment
- Does the p-medicine developer group agree with a developer audit?
- Does p-medicine allow insight into the source code?

- Does p-medicine agree to an “escrow agreement”?
- Sustainability issues that must be examined, cover:
- How is the sustainability of the product provision guaranteed?
- How will the p-medicine tool be provided to ECRIN and other users?
- Plan for the provision of the p-medicine tools
- Business model of p-medicine after the end of EU-funding (e.g. stability of financial background)
- Business continuity plan
- Can tool developers / p-medicine group provide support for the software user?
- Can tool developers/ p-medicine group maintain services for the software user?
- Can tool developers/ p-medicine group provide user training?
- Does the unit have adequate staff to provide support / maintenance?
- Is there a plan for ongoing development of the tool?

3.4.2 Questionnaire: Tool requirements for the developer

3.4.2.1 Module 1: Software development planning, code writing and use of standards

The necessity for quality in development is of prime importance for GXP. The aim is that patient wellbeeing and the quality of patient data have to be protected. The listed requirements cover the quality management at the software developer area, including:

- Existence of a software development plan (SDP)
- SOPs for the development activities
- activities for managing the requirements that are reviewed by management
- Existence of an information security policy
- Familiarity with the regulatory background (e.g. GCP)
- Familiarity with the evaluation of patient risks
- The development/maintenance/adaption of software according to SDLC is of importance as well as the employment of programming standards for each programming language.
- The standards should cover the following areas: naming conventions for files, naming conventions for variables, log-out conventions, versioning, error handling, rules for writing code, rules for lines with comments, etc.
- A review process should exist
- Processes for deviations should bespecified
- System documentation should cover system architecture, individual modules / classes and their inputs, outputs, and purposes.

The provision of a reference installation/demo installation that can be used by ECRIN members for the assessment of the tool would be an advantage.

3.4.2.2 Module 2: Quality management during development

Details about the quality management system (QMS) and the Quality Assurance activities (SQA) are evaluated in this part:
The SQA activities should be reviewed by management on a periodic basis and written policy for managing requirements should exist.
The group of developers should follow a written policy for managing the software project and for this purpose adequate resources should be available for quality management activities. Adequate resources should be available for tracking and reviewing the software project progress.
The quality management system should include a quality plan for the development of p-medicine tools, covering: roles and responsibilities, documentation standards, measures of quality assurance, tools, methods and standards used during development, etc.

Written instructions (e.g. SOPs) should be employed for: software development, change control, configuration management, review and approval of documents, support in case of software problems, supervision of the project plan, etc.
Useful Quality Control Activities cover:

- Checks for transcription errors in data input
- Checks for integrity of database
- Checks for consistency of data,
- Checks for uncertainties in data, database files, etc.
- Testing should be integrated into the development process.

Written policies should be in place and employed for the test activities, that may include functional tests, non-functional tests, acceptance tests, regression tests, system tests, etc.
Risk-based testing should be employed, that uses the risk for patient safety and data integrity to prioritize the appropriate test cases (risks of GCP relevance).
A Software Testing Plan should be employed to ensure that testing is done in a systematic way. It should cover: system characterization, incl. status of development, objectives of testing, relationship of test to risk analysis, test cases, test data, including acceptance criteria, performance, amount of testing, etc.
It is good practice to separate development, test and operational activities. Documented procedures for change control for the SDLC as well as the source code should exist and responsibilities for change management should be assigned (e.g. release of change, implementer, and reviewer). It should be possible to clearly identify each version of each configuration element.

3.4.2.3 Module 3: Generic requirements for GCP compliance of the tool

The original GCP requirements that are derived from ICH-GCP, Annex 11 and PIC/S Guide are rather general requirements, with the execption of audit trail, digital signature and access control. Therefore, this module covers these general requirements and should be seen in connection with the tool specific requirements.
Protection of privacy of patients and the confidentiality of records that could identify subjects is of utmost importance. A security system should be available to prevent unauthorized access to the tool and the data. Adequate backup of the data should be maintained and a an unambiguous subject identification code should be used that allows identification of all data reported for each subject without identifying the subject. A policy for user password management including user identification and authentication should exist.
In addition, data quality plays an important part of GCP. Thus, tools should be implemented with procedures that assure quality. In general, the tool should enable the user (investigator) to be able to ensure accuracy, completeness, legibility, and timeliness of the data reported in the CRFs or other records.
The tool should allow that data reported in the CRF that are derived from source documents, are consistent with the source documents. Any change or any correction of the data in a CRF must be dated, initialled, and explained; that is an audit trail must be maintained. In general, tools should support that all data are generated, documented, and reported in compliance with the study protocol, GCP, and the applicable regulatory requirements. For this SOPs for using the tool should be available and maintained.
GCP requirements demand the collaboration between software provider and the user. Requirements documentation (e.g. functional requirements) and test documentation, test reports, and test reviews, including document reviews, performed in the different phases of tool development (IQ, OQ, PQ) should be provided to support system validation. The test reports can become part of the validation plan.
Risk management should be applied throughout the lifecycle of the computerized system (taking into account patient safety, data integrity and product quality). In particular, developers should be able to justify their use of standards, protocols, acceptance criteria, procedures and records based on a risk assessment, including the listing of all relevant

systems / components and their GXP functionality. Therefore, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the tool. It should be assured that quality system and audit information relating to suppliers or developers software and implemented systems are being made available to inspectors (e.g. for a GCP inspection). To support this risk-based approach for critical tools / systems a description of the physical and logical arrangements, data flows and interfaces with other systems or processes, hardware and software pre-requisites, and security measures should be produced. User Requirements Specifications should be available to describe the required functions of the tool / system. They should be based on a documented risk assessment of GXP impact and should be traceable throughout the life-cycle of the tool.
Is should be ensured that the tool is being developed in accordance with an appropriate quality management system. Thus evidence of appropriate test methods and test scenarios should be demonstrated and in particular system (process) parameter limits, data limits and error handling should be considered.
Data should be secured by both physical and electronic means against any damage. Part of data security is the employment of an audit trail. Already during development it should be considered that, based on a risk assessment, a record of all GXP-relevant changes and deletions (an automatic "audit trail") is built into the system. These audit trails should also be convertible to a generally readable form and be regularly reviewed. In addition, the creation, change, and cancellation of the access authorizations should be recorded. Electronic records should be able to be signed electronically (e.g by password). The electronic signature should have the same impact as a hand-written signature; it is permanently linked to the correspondent record, and includes time and date of application.
Provisions should be in place to ensure the availability of the tool supporting critical processes, to ensure continuity of support for the processes the tool supports also in the event of a system breakdown.

3.4.3 Requirements for a CDMS / EDC system for data collection in GCP compliant clinical trials

Three tool specific questionnaires were developed: for ObTiMA, biobanking and imaging.

3.4.3.1 Requirements for Clinical Data Management Applications (ObTiMA)

A Clinical Data Management Application (CDMA) refers to the specific system established to hold the data for a single trial, plus the trial schedule and the forms for data collection instruments (eCRFs) that have been set up and validated for the trial. In contrast: Clinical Data Management System (CDMS) is the system (or collection of systems) that holds the clinical data gathered during trials. The CDMS is specialist software often purchased from vendors, but sometimes built and maintained in house.[41] We used the requirements lists created for the evaluation and selection of EDC systems for clinical trials that was developed for the KKS Network consisting of a requirements catalogue for software producers and providers (version 2001)[42] and the revised version from the same authors (2003)[43]. This requirements catalogue is based on a user survey conducted in the member institutions of

[41] Ohmann C, Canham S, Cornu C, Dreß J, Gueyffier F, Kuchinke W., et al.: Revising the ECRIN standard requirements for information technology and data management in clinical trials. Trials 2013 14:97

[42] Ohmann C, Kuchinke W, Eich HP: Catalogue of Requirements. For Software Support of Clinical Studies (with emphasis on Remote Data Entry) - for Software Producers and Providers. KKS Düsseldorf, 2001

[43] Requirements list for software for clinical studies: Catalogue of Requirements for Software Support of Clinical Studies with emphasis on Remote Data Entry. KKS Düsseldorf, 2003.

the KKS Network[44]. In addition, the newer evaluation questionnaire for CDMS vendors (2012)[45] developed by the KKSN was consulted, especially the chapter "Study Setup and maintenance".
The requirements for CDMS purchased by the KKS cover in detail requirements for CRF creation and trial data base set up. Especially, information about technical limitations were asked for: is there a limit to the number of validity rules that can be defined for a study; is there a limit to the number of users who can use the system (total or simultaneously). References and statements regarding performance of the system should exist and audit certificates, references available, reference installations and support services should be available. Support should be offered for eCRF design, installation of software updates, and error corrections. There should be regular updates of the software and a user groups should exist.

3.4.3.2 Requirements for data quality during data collection:

The software should issue an unambiguous ID for the study participants, customisation of patient Ids should be possible, options for eCRF validity checks should be offered, setting of mandatory fields, definition of tests that mask parts of eCRFs, definition of conditional branch addresses, date-time stamp for eCRFs. Furthermore, data quality can be assured by:

- Support of repeating forms (e.g. for Adverse Events)
- Support of repeating study events, meaning that the number of a "study event" depends on the occurrence of a previous event
- Does the creation of eCRFs has different steps (e.g. draft, test, validation)? CRFs can be assigned to a visit.
- Sample collection can be assigned to a visit
- Repeating visits are possible.
- Is the creation of CRFs for international trials supported? (For example: multilingual CRFs, multilingual help functions of eCRF, time specifications, consideration of time zones during data input or CRF update.
- Lab data can be shown in eCRF (e.g. as table)
- System supports the handling of incomplete date information
- Support of derived data items, meaning that the value of these data items are calculated based on the values of other data items which are distributed over a set of forms / study events of the same subject
- Change/update of eCRFs during study conduct is based on an amendment of the study protocol possible and how can this be achieved in international trials
- Which of the following supplementary functions for data monitoring and / or processing are available in the eCRFs of the software:
- Spell checking of entered text
- Automatic conversion of parameters (e.g. transformation of lab value unit into other unit)
- Possibility of annotations at the document level
- Display of protocol violations during data input
- Are the following options for data input supported in eCRFs?
- Saving incomplete eCRFs
- Saving invalid eCRFs
- Collection and display of all error messages in list format after data input
- Recording of errors

[44] Kuchinke W, Ohmann C: Nutzerprofil für Studiensoftware der Koordinierungszentren für Klinische Studien (KKS) mit Schwerpunkt Remote Data Entry - Ergebnisse einer Umfrage . Fachgruppe „Datenmanagement / Telematik" TMF, 2001.

[45] Dress J, Bessert S, Gerlach A, et.al.: Questionnaire for Evaluation of EDC-Systems. V02.12.2012.

3.4.3.3 Training and support:

Support and training for trial members, like CRA, investigator, data manager and data entry personal should be provided; as well as user support for forgotten pass words and a help desk for users should exist. Training for system administrators, monitors and investigators should be provided.
A hotline should provide some of following services: hotline in German, in other languages, in English, telephone hotline, 24-hour availability, email hotline. Training should be provided by consultants, p-medicine members, video courses and documentation, like printed documentation (manuals, etc.), media-based documentation (e.g. video) or online documentation should be offered. Support for eCRF design plays an important role; it should be possible to prepare CRFs in collaboration with p-medicine, a collection of sample eCRFs should be available.
Support should be offered for the expansion and update of the software tools, for example for the creation of new interfaces upon request, new functionalities, and CDISC support. For the maintenance of the software, error correction in the software, regular updates of the software, regular meetings, a user groups and access to websites with news, problem-solving tips,… should be available.

3.4.3.4 eCRF administration:

eCRFs are complex documents, it should be able to track/depict/search them according to: patient, site, visit / time, investigator and country. The total number of CRFs should be shown. Incomplete eCRFs should be indicated, e.g with a flag lists. The investigator should be able to sign an eCRF for approval. This eCRF approval function should be subject to country specific modifications. The system should support the import of lab data into the eCRF.
To guarantee high data quality and high usability, the system should be able to display graphic status icons for data items, forms, study events, subjects and support plausibility checks during data entry (“edit checks”), as well as plausibility checks in batch mode (“batch checks”).

3.4.3.5 Audit trail and query system:

The provision of an audit trail is one of the key requirements of GCP. An Audit Trail should record data input actions, data changes (including value before and after change), data deletions, date/time stamp and username of action and a “reason for change”. The “reason for change” should be always required, optional for defined variables, “change due to query” and must be logged. The characterisation as „Self Evident Corrections / Obvious Corrections“ should be possible. The data collection should be aided by a query system for data cleaning.
It should be possible to list queries according to: patient, site/investigator, country and the total number of queries should be shown. The creation of manual queries should be possible; and the creation of queries in batch modus should be possible. A query should be indicated as “resolved”, when released by data manager or released by monitor.
Additional functions (data sharing / coding / analysis and reporting):
The data management system should be able to support the transfer of a study subject with all data from one site to another site, the sharing of data with patient registers, provide mechansims to lock and unlock a study allowing only read access when locked. It must be guaranteed that the sponsor does not have the control of source documents and eCRF data exclusively.
The tool should offer the following aditional options for the management of patient study data: issuing an ID for each study subject, control the unequivocal assignment of ID, customisation of study subject ID, creation of pseudonyms for subject Ids, rendering of primary data anonymous / pseudonymous, selection of patients according to personal data (age, gender, place of residence, etc.). Following parameters for the administration of eCRFs

should be utilised: date/ time stamp, author logging, status parameters (e.g. cleaning status, Quality Assurance status, completeness) and source data verification code for monitor. Different types for the status eCRFs should be employed: e.g. document stored, document incomplete, data erroneous, and document complete and checked. A fully automatic status checking of eCRFs should be supported (e.g. automatic status checking with confirmation and user modification options or status checking via manual user input).

3.4.3.6 Electronic documents:

The linking of electronic documents to the data collection form is an advantage during clinical trials conduct. Some of following study related documents should be provided or referenced: patient identification, patient consent form, storage of emergency medicines, documents for specimen processing, patient-related info sheets, documents for specimen storage, patient-related labels, notification of patients regarding an examination, patient warning letters, research schedules/treatment schedules for physicians, and documents for exam scheduling.

3.4.3.7 Implementation support:

Tools that are not provided as services have to be installed at an ECRIN centre. For the installation support in different forms is necessary. An Installation Guidance including scripts for the installation testing should be provided. It should be possible to install tools by ECRIN data centre personal. User manuals should be provided for: data managers, investigators, system administrators, and monitors. p-medicine should support installation of the system in ECRIN centres as well as the validation of the system, by: provision of validation documents (requirements, test results, QA documents), test scripts and the joint conduct of the validation.
Author logging, indication of multiple status parameters (e.g. cleaning status, Quality Assurance status, completeness), source data verification code for monitor, creation of edit checks and batch checks are further requirements.

3.4.3.8 Requirements of the ECRIN Standard that apply to CDMS

The ECRIN standard was consulted to derive GCP requirements that could be used for the data management software. The ECRIN standard consists of an IT part, concerned with the general infrastructure necessary to run the data management processes of a study, and the more specifc data management part. In the data management (DM1 and DM2) sections[46] the important requirements are listed that may concern data management in p-medicine. DM 01 is concerned with the design and development of the clinical data management application. It requires that SOPs covering the development lifecycle of the clinical data management application and the CRF (incl. development, testing and deployment) should be in place . The process of CRF design should be documented, reviewed and CRF version management is employed. CRF development is performed by a cross-disciplinary team (e.g. a group consisting of programmer, trial manager, statistician, data manager) . The requirements specification for the CRF must be protocol based, including for example primary safety and efficacy variables and should consider the workflow of the trial. The CRF should be designed by using validated questions, scales and standard instruments (e.g. for quality of life questionnaires and it should not duplicate data (e.g. no redundant questions or calculate unnecessary result. Functional specifications for the CRF exists, identifying each data item on each CRF page (including field names, types, units, validation logic, conditional branching) . Procedures should be implemented that check (e.g. edit check) data input into eCRF. The usability: The usability of eCRFs should be evaluated and assessed before the

[46] Requirements for GCP-compliant data management in multinational clinical trials. Additional file 1 Standard requirements for GCP- compliant data management in multinational clinical trials

deployment. For this purpose, CRFs have to be reviewed against the protocol, end-user expectations and CRF design best practice. At the end an acceptance test for CRFs is conducted.
Common documentation principles should be 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.). Quality documents covering good design practice, usability, local design conventions, etc. should be available
Clinical Data Management Application Policies for clinical data management application and CDMS validation should be in place; a trial-specific Test Plan covering scope of test, item pass/fail criteria, etc., the testing with sample data against functional specifications testing of all validation checks and conditional data capture mechanisms should be conducted. A Validation Report should be created and signed by responsible DM person, as well as the CRF Approval that has to be signed off by key persons. The Validation Program should consist of lists and scripts; results are documented and retained. The process of clinical data management application design and data checks programming is validated against specifications. A defined way of Change Management of Clinical Data Management Application should be followed; SOPs and policies for clinical data management application change management should be in place. Any amendment is tested in a test environment, following test specifications and the test results are recorded. In the case of significant changes, the need for re-training is evaluated and mechanisms exist that easily inform relevant staff and users of changes, and provide support. CRF page numbering and version information is always updated.

3.4.4 Requirements for a tool to support biobanking in clinical trials

3.4.4.1 General management and study set-up

We assume that the biobanking tool will be used for a clinical trial. Therefore, the tool should be able to create user, centres, institutions. The best approach is that biosampling is integrated with the clinical data management system (e.g. EDC system). In this case input of biosamples information in the eCRF is possible. Institutions should be able to assign centres (sites). With the tool it should be possible to set up a new clinical study. In each study the number of collected samples as well as the complete storage time of samples should be indicated and the system should be able to consider sites of a trial, containing information about: the leading investigator, study number, study start, study end, participating countries, participating sites, date of last update, site ID, contact information, number of enrolled patients, date of first patient, first visit, date of last patient, last visit. The system should be able to capture automatically the current date and time.

3.4.4.2 Sample acquisition / check in requirements

The first step in biosampling is the sample acquisition. The system should allow users to upload and associate signed informed patient consent forms with biological sample records. For this purpose, the system should have a link/reference to the patient informed consent and the system should support the creation of informed patient consent form templates which are in a language understandable to the subject (or their representative), list all research projects for which the biological samples will be used, address the future use of the samples (including commercial use and unspecified use), provide information about the release of individual research results, and provide information about the possibility of consent withdrawal or later modification.
In general, the system must allow authorized users to enter new biological sample records. In addition to compulsory sample data, the system should allow users to enter the following data when importing biological samples: identifier, depositor's name and address, source, substrate or host from which the biological material was isolated, geographical origin of material, growth media and conditions, cell preservation or storage conditions where known and hazard information.

The system should support the process of patient / donor anonymisation. This is done in our model in two steps. The process of anonymization and its review must be logged by the system.
First, the generation of a pseudonym and a barcode (BC1) should be possible. Second, the system should be possible to generate a second pseudonym for a second barcode (BC2).
The system should manage the check-in of patients, including following information: availablity of informed consent, BC1 search, BC1 as well as BC2 is checked for validity, and following information is checked: date of visit in centre, type of sample (blood, serum, tissue, others...), sex of patient. After the check-in of new samples a new pseudonym and corresponding barcode is craeted. BC2 is generated and replaces BC1. It must be guaranteed that the assigned BC is not used again in the study.
When a new trial is created the system should guarantee that for each trial the number of samples to be taken out of storage as well as the complete storage time is indicated. For this purpose, following steps should be managed: pseudonymisation of barcode 1, check-in of patient, check if an informed consent is available, BC1 search, check for validity of BC1 as well as BC2.
In this way the system guarantees that samples of trial subjects are coded threefold:
Study participant number (study ID, patient number)
First pseudonym (BC1, barcode 1)
Second pseudonym (BC2, barcode 2). The sample is stored only with BC2.
At the beginning, the tool should allow the generation of an unequivocal patient number: every patient study ID is used only once in the system, this is checked when a new ID is assigned. But the check-in of patients without IC entry should be possible. The system should be able to guarantee that every sample can be identified only by its BC2 (second pseudonym).
The system should be able to generate an inventory list of all samples collected for a study, in a country, per site or per patient. There should be no limit on the number of BC codes possible.
The system should allow that a patient withdraws from a study, including the deletion of patient number and corresponding samples. During patient check-in the system checks the validity of the informed consent. The system may request informed consent information. During patient check-in the system checks that all patients of a study have been assigned to a site. The system supports the pseudonymisation of patient informed consent and a patient's informed consent can be deposited in the system.
The system must be able to track the physical location of samples by allowing users to associate the following data each sample: location, container, etc. and the system should allow users to track the movement of samples by recording data like: current location, a predefined number of previous locations, date moved from last location, date received at current location, person responsible for the move.
The system should support the validation of biological samples by allowing users to record details of the validation process, including data like: location of the validation, list of items validated, customer name and address, date of receipt of items to validate, date of validation, type of action carried out on the sample (e.g. purity check, quality check, identity check), validation results with units of measurement, abnormalities observed, and person responsible for the validation results.

3.4.4.3 Selection / Requests for samples / Retrieval

A process for request and selection of samples should be implemented in the tool to enable a sample request. Upon request a list with following information should be generated: study, CSR, number of samples, name of analysis / extraction, due date, etc. After sample request, a list is generated covering all samples of the request with information like: SGN, BC2, material, amount, units used, status of sample, and status of process. For a request a list with selected BC2s is send to the sample manager and the sample manager finds and

checks out the requested samples from the biobank. A trustee should be able to search for patients, but only for patient number or BC1. The system should support sample retrieval. It should track all requests for sample retrieval. This includes recording data like: date of request, list of samples requested, person who requested samples (investigator), purpose of retrieval (study).

3.4.4.4 General system requirements and interoperability

An interface with a biobank management system should be supported to simplify the management of samples. Several steps during trial conduct with biosampling will be supported by the p-medicine tool, other by the biobank. The system should be able to create new users; only the administrator should be able to activate and deactivate users and to assign following roles:
Clinical site: data manager, process controller, auditor
Lab: administrator, sample registrar, sample manager
The system should create a list of all users. The role of trustee is able to make changes in the system concerning the informed consent of patient, but only when patient expresses wishes for a change in written form. The system must allow authorized users to export: sample records, and a catalogue of sample records and the system should create a log of all export operations.
The system should also be able to import sample records, and records of other entity types, whereby imported records should be subject to a data validation step.
The system must be documented in sufficient detail, including functions, fields of data entry forms and appearing errors and possible solutions, etc. To support usage, the system should provide an online help covering context sensitive or visual guidance. The system should assist the user during data entry by following measures: suggest possible text values, drop down menus when possible, provide default values, etc.
The system should be possible to generate error messages or alerts; error messages must be meaningful, so that users can decide how to correct the error or cancel the process.
System recovery must be possible. The system must provide an automatic backup feature, and a recovery feature for restoring entities from backup files. The capability of data backup by the system must be checked regularily.

3.4.4.5 Security issues

The system must record the following data per log: action, entities involved, user undertaking action, date and time of action. In addition, the system should record automatically all critical actions in an log, like actions which result in the deletion of entities, anonymization / pseudonymisation, data modifications, user management actions, user authentication attempts, any access violation attempts, all changes to log settings. The system must not allow users to access the tool without authentication.
The system should support the authentication of users by ID and password. The system must ensure that the data entered by the user during authentication cannot be intercepted by third parties. The system should log both successful and unsuccessful user authentication attempts. In case the system receives an unsuccessful user authentication attempt, the system must not reveal any information about the validity of the user ID.
To protect any health information of patients, the system should adhere to privacy laws. The logistics for a withdrawal of consent must be clearly defined and conveyed to all subjects at the time of consent. Anonymization should be verified by an appropriate review procedure.
The system must support the management of information related to the following sample lifecycle processes: sample acquisition, including sample collection and receipt of samples, storage of samples and associated data, processing of samples, disposition, selection, retrieval of samples. The system must prevent users to associate identifying data with non-identifiable biological samples. In the described model, the system guarantees that no role

except „sample registrar“ or „code exchanger“ has access to the patient number or BC1. The system should test whether the input value matches the format specified for the given field
The system should allow authorized users to access: sample records, procedure records, documents (e.g. informed consent), storage unit records, user records. The management of centres (sites) should be possible containing information about: number of participating sites, number of planned patient recruitment, status of study, number of collected samples.

3.4.5 Requirements for the evaluation of Dr.Eye for clinical trials usage

3.4.5.1 General aspects and system limitations

The components of the imaging system and if they are web-based modules as well as their functionality should be listed. It should be described how the system supports image handling during the conduct of clinical trials.
The system should allow image handling during multiple trials at the same time (e.g. manage different user accounts across different trials). The limits of the system should be clearly stated: limit to the number of trials that can be conducted, limits of the number of images that is supported, limits in the size of the images.
The structure and the components of the imaging system? Should be described: integrated picture archiving system (PACS), web-based picture archive system, connection to a clinical data management system (CDMS, EDC), imaging amendment tool, DICOM viewer, image processing unit, portal or web entrance (a single access unit for all study participants), image review unit, image analysis unit, data extraction unit, image transfer system, or others. The description should state if how the system interact with a PACS.

3.4.5.2 Quality aspects of imaging in clinical trials

The system should check the quality of incoming images; it should support the use of validated standardized image analysis techniques. The system should support the standardized extraction of quantitative image information. Validated and standardized image processing techniques should be used.
The ensurance of image quality is an important requirements. In detail, a loss-less transfer of information (imaging data) shlould be guaranteed. The system should generate transfer protocols. A centralized analysis of imaging data should be supported. Validated DICOM protocols should be used to ensure a lossless transfer of images via internet. The upload of an image data set should be accompanied by a quality check that assures that the data set fulfils the trial rules, e.g. regarding patient anonymity of the image meta information.

3.4.5.3 Process aspects of imaging and standards in clinical trials

The electronic transmission of imaging data between different sites and the central repository should be supported. The combined management of imaging and numerical and other data by linking image storage with the clinical data management system should be possible. A high availability (site independent) and well-structured access to data, images and trial results should be ensured.
It should be possible to specify rules to be set up for individual studies, for example, to ensure a consistent use of information in DICOM tags. For this purpose, the system should allow the definition of data items or data item groups that become editable or visible only if a predefined condition is met? Numerical analysis results should be able to be exported into a CRF. Investigator should be able to input own clinical trials images / clinical imaging data. Images should be send/received by the investigator from any personal computer.
It must be described, if a central image repository for the clinical trial is available, or if local image repositories are used. The transfer, up-/down-load and viewing of imaging data via internet from a local personal computer to/from a central PACS should be possible. Images should be sent / received by the investigator from the local PACS to be used by the tool?
The tool should support image post-processing and analysis. The tool should support the joint usage of CDMS/EDC, PACS and image processing tools. For this purpose, the tool

should allow for searches in the imaging data bases and it should be possible to call PACS and the image processing unit from the clinical data management system (e.g. EDC system) for cross-linking of data and for enabling semantic searches in the database.
The following environments for image handling should be established and managed within the application: development, testing, validation, training and production / operation.
The tool should provide imaging data with expert annotations; metadata should be managed and images should be tracked/depicted/searched for according to: patient / PID, trial site, visit / time, investigator, country, total number of images uploaded.
The tool should support imaging review and provide image approval functions. Corrupted images should be flagged? A status should be assigned to images (e.g. image reviewed, image analysed)? Ideally the system would display graphic status icons for the images.
Open standards in accordance with the Integrating the Healthcare Enterprise (IHE) as well as established standards such as DICOM, HL7, and XDS should be supported.
The system should enable image retention. For this purpose, policies, especially security policies, should be provided. The system should generate alerts automatically, e.g. for outliers or according to specified criteria. It should be possible to send alerts via email, text, system messages. It should be stated, if the PACS or another database can be used for long-term archiving of study images after the end of the study.

3.4.5.4 Data security and data protection aspects

The access to the data base / imaging repository should be controlled. Each user of the tool should register for a user account before using the system. All privileges and access rights should be controlled via user accounts, e.g. it should be specified who is allowed to upload and download data/images, and access certain images. In general, data protection (privacy) should be guaranteed by the tool. The system should support following security relevant methods: https, secure web-protocol, eligibility check of users, each user has only access to assigned data, during the image up-load, all private header information will be automatically removed and replaced by a pseudonymous patient identifier (PID).
The tool should generate pseudonyms or interact with a tool to generate pseudonyms (e.g. PID generator). Imaging data should be transferred through the internet only in pseudo-anonymous form; storage of all data / images should be done pseudo-anonymously. It should be possible to encrypt the pseudonym (PID) during transfer via internet and during storage. It is possible to integrate a trusted party (TTP) in the operations of the tool; thus in case the tool generates pseudonyms (PID), these will be located by a trusted party (TTP).

3.4.5.5 Training and support

Can support and training for CRA, investigator, image reviewer, image analyser and data managers be provided? Exists a user support, a help desk?
User support for forgotten passwords should exist. The system should offer integrated help functions. Training for system administrators and users should be offered. Some of following support and / or hotline services should be provided: hotline in German, hotline in English, telephone hotline, 24-hour hotline availability, email hotline, training by consultant, training by p-medicine members, online documentation.
User documentation should be provided for training, including printed documentation (manuals, etc.), media-based documentation (e.g. video), online documentation. Support for the expansion and programming of the software, like new interfaces created upon request, new functionalities, new analysis algorithms, image analysis validation.
User manuals / SOPs should be available for data managers, investigators, image reviewers, image analysts, system administrators, monitors and others. p-medicine should be able to support system validation of the imaging system in an ECRIN centre.

3.4.5.6 Platform and security requirements

It should be specified what web browsers can be used and which browser features are mandatory, like Flash or Java Script. In general, image data transfer should be encrypted?
It should be specifies if the tool can be hosted, at a ECRIN data centre or by p-medicine, or by an independent hosting provider. The system should offer a well-defined and stable application interface (API), which can support interoperability with other systems. The password and log-in features should cover: minimal password length, forced password change after 1st login, forced password change after defined time, defined complexity of password, recording of password history, minimum of changed characters, restricted number of failed logins.
Integrated into the software should be the encrypted sending of usernames and passwords, encrypted saving and storage of data and images, a backup-restore system (e.g. secondary hard disk, DVD), crash protection (hard-disk imaging) and that the loss of connection triggers automatic log-off.

3.4.6 Conducting the interviews

The questionnaires were created and distributed to developers at USAAR, FORTH, Fraunhofer IBMT und UCL (Fig. 2):

- USAAR, development of ObTiMA and the biobank modul of ObTiMA
- FORTH, development of Dr.Eye
- Fraunhofer IMMT, development of Biosample Manager
- UCL, development of imaging and data warehouse

The questionnaires were completed by self-reporting by developers. For the assessment of ObTiMA a structured interview with the USAAR developer was conducted at UDUS (28.11.2013); telephone conferences were made with FORTH (17.12.2013) and Fraunhofer IBMT (19.12.2013). After the telephone interviews, the answers given were ammended with comments and revised. UCL did not complete the questionnaire so far and did not participate at a telephone conference. A telehone interview with N. Graf (USAAR) about the business plan for p-medicine was held 29.4.2013. A joint meeting of p-medicine and ECRIN was held 30.4.2013 that dealt with p-medicine/ECRIN cooperation and GCP compliance of p-medicine tools (especialy ObTiMA) and potential business models of p-medicine.

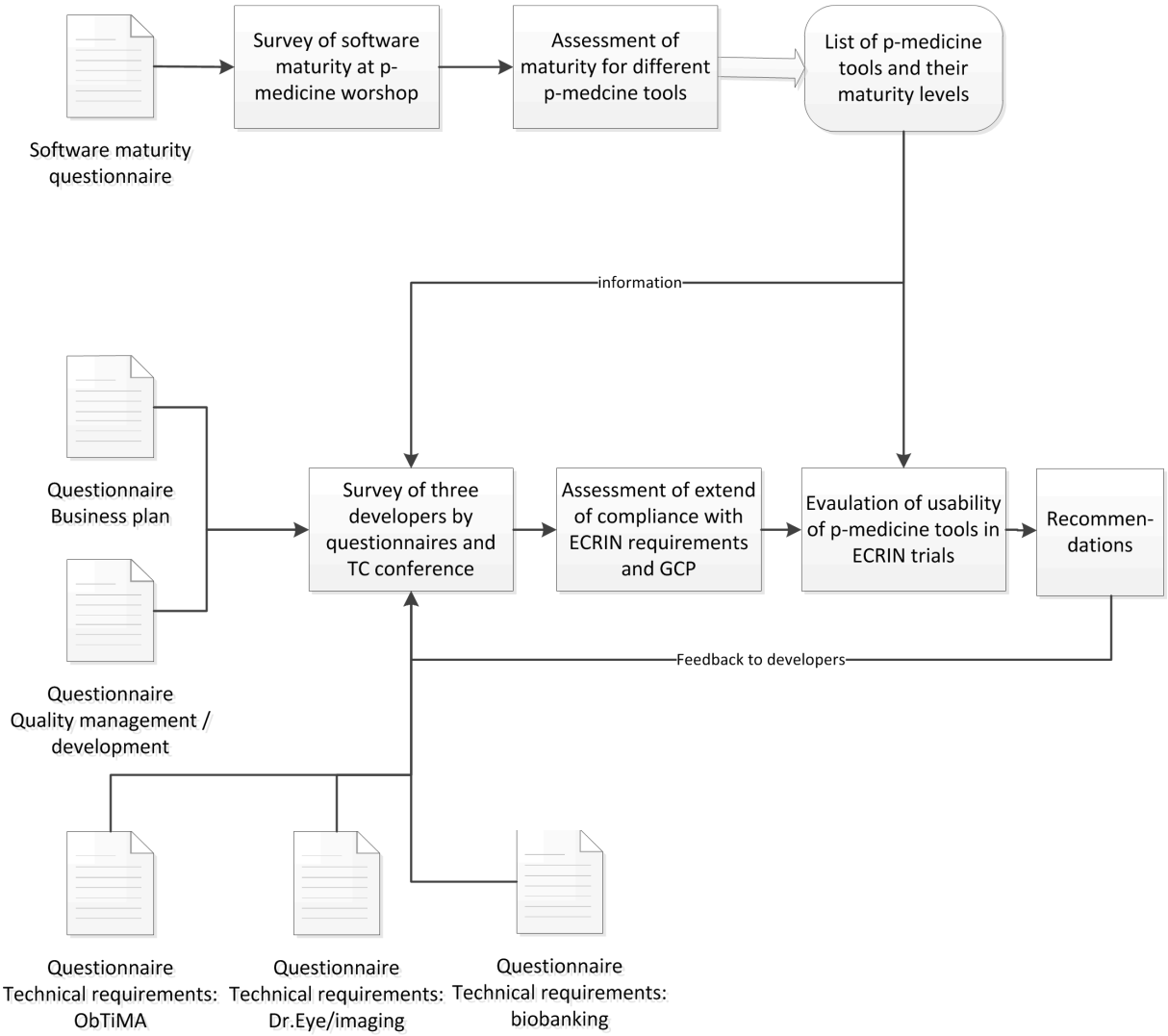


Fig. 2: Structure and interdependencies of maturity analysis and evaluation surveys

3.5 Gap analysis (Evaluation of p-medicine tools / services)

In general, a “gap analysis” is developed to measure the gap of service and tool delivery with the expectations of the customer[47]. Gap analysis is a strategic management tool to analyse and quantify an “as-is state” with an “expected or envisaged state”. For this evaluation report of the usability of p-medicine tools within the ECRIN infrastructure, the gap analysis approach was adopted and adjusted to the difference of the current state to the requirements for usability. In this way, we used the gap methodology to analyse die differences between the requirements and specifications for compliant clinical trials with that what p-medicine tools have to offer.

p-medicine project aims to build a sustainable environment for p-medicine tools/services. Thus, there is an urgent need to transform p-medicine from an academic driven project to a fully operational, professional and business driven organisation with a portfolio of services and products. This transformation process needs an alignment between p-medicine

[47] Parasuraman,A. ,Zeithaml,V.A. and Berry,L.L. (1985) A conceptual model of service quality and its implications for future research, Journal of Marketing, 49, 41-50

management's strategy and the envisaged customer needs, such as ECRIN. The evaluation and the gap analysis focus on following questions (Fig. 3).

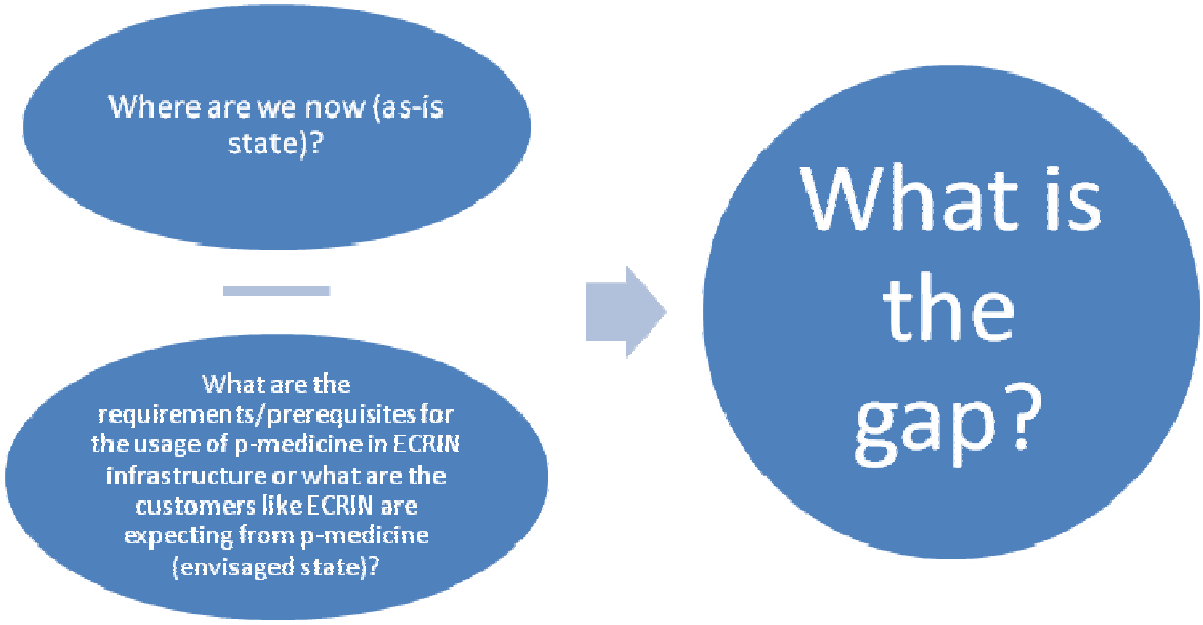


Figure 3: Gap Analysis Approach

In a first step a maturity based evaluation model has been used to assess the tools maturity level (see chapter 3.1). Further questionnaires were developed to assess and identify the business, quality management and development aspects (see chapter 3.4). Based on these three questionnaire's self-assessments, the as-is state was identified and compared with the requirements for compliant system use in ECRIN trials (envisaged state). For each requirement or specification, the degree of implementation was assessed (implemented, partly implemented, not implemented, not applicable). Aggregated evaluation criteria and the results of self-assessments were mapped and assessed (see chapters 4.3.1.7 and 4.3.1.8) and observations were derived (see 4.5.2) and qualitative gaps identified.

In this way, the identified gap was analysed and recommendations were established to engage p-medicine's management to "close the gap", respectively to increase or to increase the usability of p-medicine tools/services within the ECRIN infrastructure (see chapter 6.1).

3.6 Evaluation/Analysis of the Self-Assessment Results

The self-assessment questionnaires were developed to meet a broad range of requirements in order to get a better understanding of the developed p-medicine tools/services. The first step was to structure and condense the large amount of requirements to make the results easier to analyse. An evaluation sheet (Appendix 7.3) was developed that contained 36 criteria from the "Quality management and GCP questionnaire". 23 criteria were mandatory for tool usage in ECRIN. Criteria were further organised according to six main compliance areas:

- Development practices (covering: requirements for SOPs, specifications, source control, testing,…)
- Validation (covering: requirements for (covering: requirements for CSV)
- Non-functional requirements (covering: requirements for security, access control,…)
- Regulatory compliance (covering: requirements for GCP)

- User support (covering requirements for: support and training)
- Ongoing development (covering: requirements for bug fixes, test scripts,…)

For each of these categories mandatory and optional requirements were identified and assessed (not met = -, partially met = o, fulfilled = +). For each requirement that was partially met or not met, observations were made based on the self-assessments of the developers. These observations and the knowledge of the p-medicine project build the basis for recommendations on behalf of ECRIN (see 6.1).

For ObTiMA/Dr.Eye nine main areas were created:

- QA
- GCP compliance
- Security
- Training
- Support
- Maintenance
- Availability
- Stability

Results of the survey are shown in chapter 4.3.1.6 and used for the development of recommendations for User Support. The results of the tool specific classification are shown as tables: chapter 4.3.1.7 for ObTiMA and chapter 4.3.1.8 for Dr.Eye. For the Biomaterial Manager questionnaire was completed incompletely, because a large part of the development takes place at USAAR to create the biobanking module of ObTiMA. In a next step analysed results were phrased as statements, evaluated in light of usability for ECRIN and used to create recommendations.

3.7 Feed back of results into Del15.3 for validation procedure

The results of the gap analysis and the risk assessment can play an important part for WT15.4; they can form the basis for the validation of p-medicine tools (WT15.4). Gap analysis as well as risk analysis created criteria for GCP compliance of software products for clinical trials. The gaps point to these features that still need improvement to reach a compliant status. WT15.4 will address these gaps to create strategies and corrective actions to allow for a complete validation of all tools.

4 Results

4.1 Status of the developed tools

4.1.1 Different degrees of maturity

In the p-medicine project, the tools and the associated infrastructure is built as modules by different developer groups. Therefore, in a first step the maturity of the software development of p-medicine tools was assessed. We used the concept of software release life cycle with a defined sequence of software development stages[48] (Fig. 1 and Tab. 1). To assess the maturity of a software tool, different degrees and a rating (see appendix) for the given answers were defined. As a result of the software maturity questionnaire a subset of three different degrees emerged. These three degrees attached to the tools are: alpha, beta and release candidate (Tab. 1). The table shows the characteristics of the three stages and corresponding reference documents that are created in each of the stages.

Stage	Maturity	Specifications and documents
Alpha	Unstable, raw source code, subset of basic functionality, data loss, proof of concept	Core requirements specification, rudimentary software development process, software design, raw source code, test scripts + data (white box testing)
Beta	Basic functionality, unstable, performance/ speed issues, data loss, usability issues	QM, software development process, delivery process, change-request-management, feature set, bug tracking, usability tests, test plans (black box testing)
Release Candidate	Basic functionality, minor bugs, feature set completed/ closed, code completed	Closed feature set, user manual, installation procedure manual, operational procedure manual, process procedure manual, test scripts + data, assessment of usability
Release candidate	Version implemented in a productive environment	Full validation documentation

Table 1: Emerge degrees of software product maturity

In structured interviews based on a questionnaire, developers were asked about their tool development.

Tool	Maturity status
ALGA-C	ß
Data uploader	α
ObTiMA	RC
Ontology Annotator	ß
p-BIOSPRE	ß
Biomaterial Manager	ß
Workbench/Portal	α

Table 2: Maturity status of seven p-medicine tools (RC=Release Candidate)

[48] http://en.wikipedia.org/wiki/Software_testing; http://en.wikipedia.org/wiki/Software_release_life_cycle

The results were analysed using the software release life cycle. The assessment of the questionnaire disclosed a more detailed overview of the stages of the developed tools. It showed that only ObTiMA is in the advanced status of release candidate. The other tools are either still alpha or beta (Tab. 2). In general, the matutity status of the different tools differ considerably.

Out of this assessment, a heatmap (Fig. 4) were created to depict visually the results of the survey and the stages of the tools. The heatmap can give an overview what is already implemented and what is missing. Zero (red) means that no requirement is met and five (green) says that all requirements are met ("the hotter the point, the more the tool is in need of improvement). Whereas ObTiMA looks quite good (large green area), with quality documents, testing and continous delivery more or less in place, Workbench and BioSPRE seem to lack behind in their development. Workbench has large orange areas and BioSPRE lacks testing and continous delivery (red). Biomaterial Manager and Ontology Annotator too, need further development in the areas of continous delivery and testing. In summary, both testing and continous delivery are the activities in need for improvement for most tool developments.

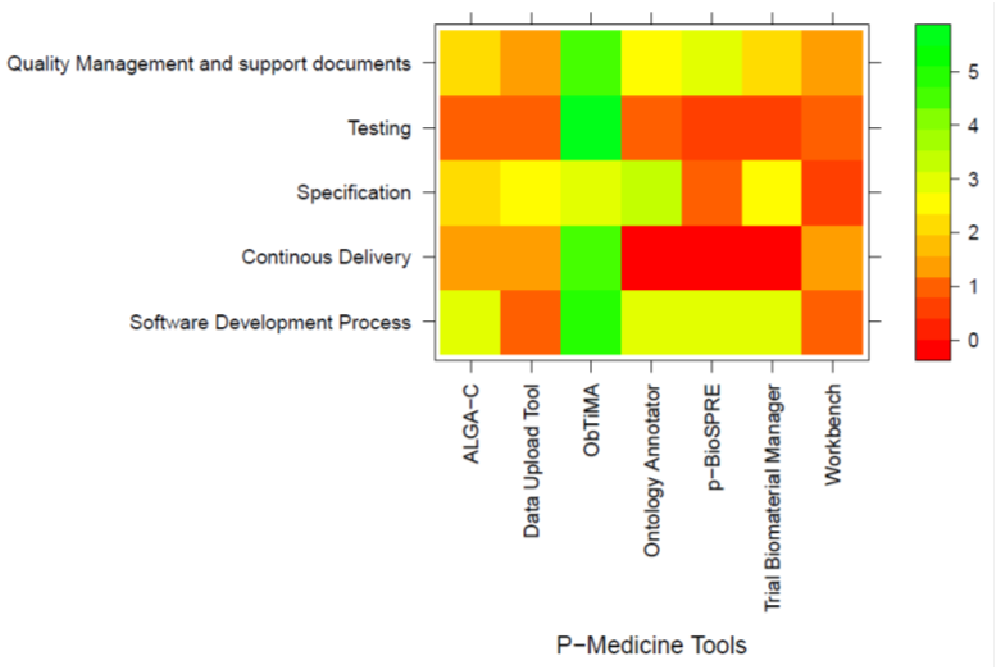


Figure 4: Heatmap of the tool maturity (Scale: 0 (red) = no requirement is met, 5 (green) = all requirements are met

As a result of the assessment, a wide distribution of different maturity stages were detected. None of the tools can be employed to date in a clinical trial. Whereas ObTiMA already is in a quite advanced states and needs mainly additional specifications, all other tools have to be further developed and tested. For the further assessment of the usability of p-medicine tools, we therfore concentrated on ObTiMA that can be used for all kind of trials and added Dr.Eye for imaging and Trial Biomaterial Manager for biobanking to cover clinical trials in personalised medicine. Dr.Eye[49] was not included in the maturity assessment, but has been independently developed to an already mature stage.

[49] http://p-medicine.eu/tools/dr-eye/

4.1.2 Consequences for the evaluation of the usability in ECRIN trials

The high degree of hererogenity in the maturity stage of the tools has consequences for an employment of all tools in clinical trials (Fig. 5). The figure shows in a generalised way the consequences of differences in the development of tools for the subsequent release and provision phase. Integration of the tool and coordinated preparation for the release will become major efforts. Only a Live release will be validated for GCP compliance to be employed in clinical trials. In its present state no tools has the degree of maturity that would allow an employment in ECRIN.

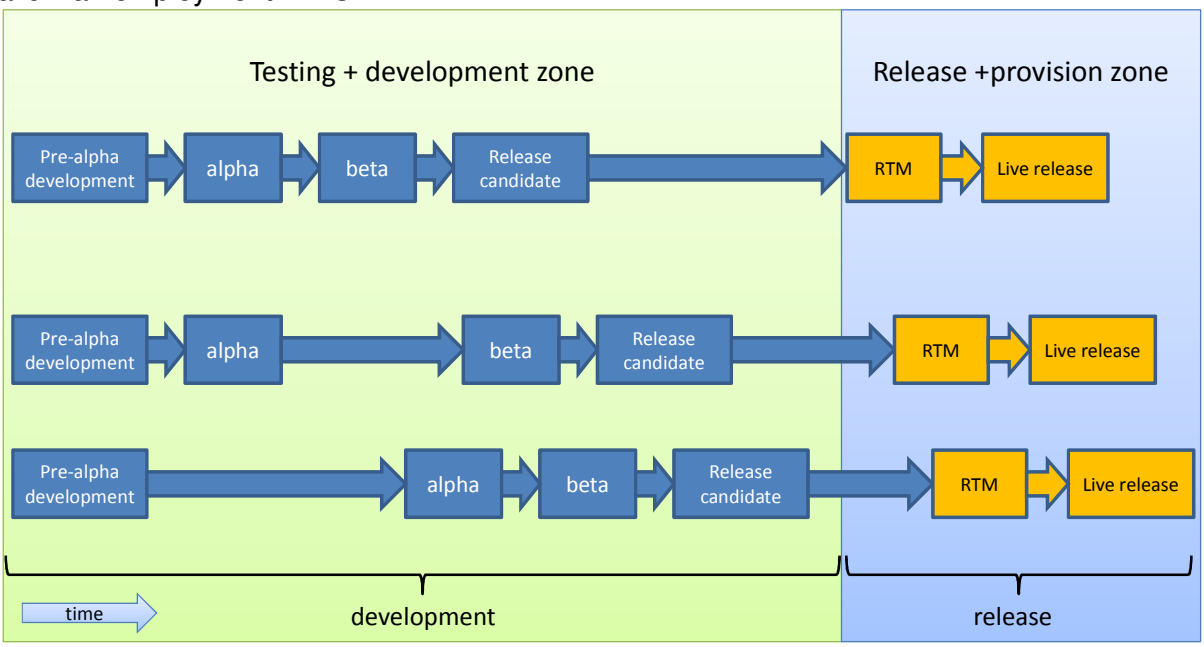


Fig. 5: Release live cycle and different maturity levels of three generic p-medicine tools (RTM=release to manufacturing/marketing). Indicated is a delay in the Live Release. The diagram illustrates the general problem of time-delayed development.

As a consequence of the differences in the assessed maturities of the developed tools different approaches to support the development process was discussed. One supportive activity is to provide developer training that is adapted to each of the different maturity levels. Because each maturity level has to fullfill different quality and compliance requirements, different training subjects have to be addressed (Tab. 3). All training of the higher maturity levels have to include training of the quality requirements of the lower levels. According to the maturity degree, different topics are trained to enable developers to generate necessary documentation and quality tests necessary for validation (Validation simulation).

	Topics of the training (additive)	ECRIN aspects of involvement
Alpha	Definition and scope, roles and responsibilities and the description of each tool, Software requirements specification, Vendor assessment questionnaire, System design, Traceability matrix	

Beta	Installation Qualification (IQ), Operational Qualification (OQ), Set of test scripts and scenarios, Defining the areas and systems to be validated, Providing a written program	
Release Candidate	Integration strategy, Rollback strategy, Data integration concept	Training/ education, Hotline/ contact, Maintenance, Internationalisation, GCP requirements

Table 3: Topics of training of quality requirements to produce documents necessary for validation (Validation simulation)

The next step was the gap analysis of anwers (reqiorements), which is a technique to determine what steps need to be taken in order to move from the current state to its desired, future state.

4.2 Assessment of the requirements

4.2.1 Results of the developer interviews

4.2.1.1 Business continuity and sustainability of p-medicine tool provision

The usability of p-medicine tools has an important business aspect; p-medicine tools must be affortable and their sustainable provision must be guaranteed. Here the problem how p-medicine tools will be provided after the EU funding phase. Strategic planning will enable p-medicine to further develop the tools and to provide robust, error free solutions to the research community that meet the needs of a changing research and funding environment. A method to analyse the market for a tool is the SWOT diagram to analyze strengths, weaknesses, opportunities, and threats for p-medicine tool provision in a cohesive format.
Telephone interviews and a joint p-medicine/ECRIN meeting provided information about the business plan for p-medicine. In principle, p-medicine tools can be installed at a ECRIN data centre, provided as ASP (application service providing) hosted at p-medicine, or provided as SaaS (software as a service) hosted at p-medicine. All three scenarios are possible for p-medicine and no decision has been reached yet. For example, ObTiMA could be offered as a Open Source tool for the core components (data collection); the additional modules for biobanking and imaging could be offered for a fee. Important is that for each tool a value proposition should be developed to see who the potential users of the tools are. On the other hand, the pseudonymisation service is provided by Custodix[50] and this SMS has an own business plan. Custodix's business model must be seen separate from the one of p-medicine; and ECRIN may use not Custodix for the pseudonymisation service but another provider.
In one scenario ObTiMA is hosted centrally and offered as ASP for example as SaaS. For the usage of the tool, ECRIN could pay a fee, or ECRIN could provide own services to p-medicine (e.g. training/support) to reduce the fee. One business model is to allow free usage of the tools for academic users, and require a fee only from phrama industry users. To support a viable business proposition, it will be of utterly importance to show that p-medicine can be efficiently and affortable used in clinical trials.

[50] https://www.custodix.com/

STaRC (Study Trial and Research Centre)[51] has been created at the "Universität des Saarlandes" that aims to develop and provide IT tools for clinical cancer studies, clinico-genomic trials and translational research. After the end of the p-medicine project STaRC may be hosting p-medicine tools; thereby addressing the question of sustainability. STaRc could become a legal entity for the provision of services and tools[52]. One possibility is that STaRC could become certified as an ECRIN data centre.
In summary, tool provision for trials in personalised medicine is an uncharted field. To become truly usable for ECRIN and other customers, a convincing business model is needed that can ensure sustainability.

4.2.1.2 Results of quality management and GCP questionnaire (ObTiMA, Biomaterial Manager and Dr.Eye)

The description of the developer group shows that all are developing in an academic environment, this is software as a project and not software as a product. Thus, on the one hand ObTiMA is a software within research projects (newest technologies for semantic interoperability), on the other hand, the development follows another focus, to develop a stable tool using industrial methods.
Developer work at the main components (that is the industrial focus, together with part-time developers coordinated). Additional expert may participate, for example in the design phase.

	Requirement / specification	Result of developer groups of ObTiMA / Biobanking / Dr.Eye
1	Is a conventional or agile approach used for software development?	All three groups use an agile approach that is based on frequent meetings. Two specify an Scrum like approach
2	Organisation of the agile approach (for example, exist product owner, scrum master, meeting schedule)	Frequent, nearly daily meetings of the group. One group specifies monthly sprint meetings, another group uses JIRA. For ObTiMA Norbert Graf (USAAR) und Stephan Kiefer (IBMT) function as product owner.
3	Does a software development plan (SDP) exist?	Two groups have a (software development plan) SDP, one does not
4	Do developers participate in training?	In two groups developers did not participate in training lately, in one they participated
5	Are members of the software group trained to perform their development activities?	Members of all three groups are trained to perform their development activities. One group specifies the training as internally.
6	Do SOPs for the development activities exist?	In none of the groups development SOPs are in use. Development practices are based on Good Practices, and conventional practices that developers use and that are trained. No formal written controlled documents exist.
7	Existence of an information security policy (ICP)	No formal ICP exist; but information security is

[51] http://eu-starc.eu/
[52] Graf N.: STaRC (Study, Trial and Research Centre: Structure, aims, tasks and perspectives). Presentation, 30. Apr. 2013 in Paris.

		considered during testing and development.

10	Information security awareness, education and training	This requirement was not really understood. In two groups information security awareness exists, in one not. It is seen as an internal requirement.
11	Do developers have knowledge/experience with testing and validation of computer systems (e.g. previous audits, inspections)?	All groups answered with yes. Testing is done in all three groups.
12	Reports of previous audits or inspections	This requirement was not really understood. It is concerned with an GCP assessment of the developer group by a software user. No such assessment has been done in any of the groups.
13	Familiarity of developers with the regulatory background for software for clinical research (e.g. GCP)	All three groups are familiar with the GCP background. The ECRIN standard is mentioned as one source.

14	Is software developed /maintained/adapted according to SDLC (system development life-cycle)?	In one group this is the case with the steps for bug tracking, feature requests, audit, etc.; in two groups this is not the case.
18	Use of development standards	Two groups are using development standards, one does not. Standards are used for naming conventions for files, naming conventions for variables, log-out conventions, versioning, error handling, rules for writing code. No standards exists for line comments.
22	Are written policies in place and employed for document review?	All three groups don't use written policies with document review. Policies exist for example for code review, but that are no controlled documents.
23	Is there a unique definition, which documents underlie a review process?	None of the three groups don't as a defined review process established.
24	How is the review process organized?	One group has a review process, two have not. Review is done on an ad hoc basis. Though the process is defined, it is not fixed in writing.
25	Are processes for deviations specified?	In two groups processes are specified, in one not. Processes exist, but are only implicitly specified.
26	Is system documentation that covers system architecture, individual modules / classes and their inputs, outputs, and purposes developed that can be provided?	In one group system documentation exists, in one group not, in one group only partly.

33	**Reference installations** for separate phases: e.g. initial installation, then test phase use and routine use	In one group several reference installations exist, in the other two groups none exists.
34	Are written policies in place and employed for integrity tests, security checks, patches and updates that are security relevant?	Two groups do not have written policies, one group has. Usually policies are conventional; agreements exist, but not in writing.
35	Are written policies in place for emergency precautions?	Two groups do not have written policies, one group has. Agreements exist istead.

36	**Software Quality Assurance (SQA)** activities	SQA activities were indicated mainly for one group. This group uses bug tracking, SVN (subversion) for version control, nightly installations, library and Test Builds for continuous integration are employed
37	Review of Software Quality Assurance (SQA) activities by management	SQA activities are not reviewed by management in all three groups. No QM handbook exists to define such activity. But for example, code checking is done regularly. Development head may act as a reviewer for code checking.
38	Are software quality assurance activities trained?	No formal training exist; training is done at the job by peers
39	SQA review of the activities and developed products of the group	In one group SQA review is conducted, in two group not.
40	**Written policy** for managing requirements	No written policies exist; conventions / agreements are used.
41	**Written policy** for managing the software project	No written policies exist; conventions / agreements are used. Policies are followed especially for java feature request, bug tracking, requirements change, feature handling, etc.
42	Written policy for software configuration management	No written policies exist in all groups
43	Written policy for employing and maintaining a standard software development process	No written policies exist in all groups
44	Written policy for training	No written policies exist in all groups
45	Written policies for a developer audit by ECRIN	No written policies exist in all groups
46	Are adequate resources provided for quality management activities?	No written policies exist in all groups

47	Does the quality management system include a **quality plan** for the p-medicine project, covering: roles and responsibilities, documentation standards, measures of quality assurance, tools, methods and standards for development, code review,	In one group such a quality exist, in two groups not. The quality plan is not obligatory (like a contract), but every developer follows it by arrangement

	traceability?	
48	**Written instructions (e.g. SOPs)** for: software development, change control, configuration management, review and approval of documents, support of software problems, supervision of project plans, storing and archiving of quality relevant documents, archiving of software (source code), management of problems, user access and physical/logical security • Handling of complaints • Performance of audits by customers?	Written instructions exist in none of the groups. Though, descriptions exist for checks, testing, configuration management, but not as controlled documents
19	Quality Control Activities, for example: check for transcription errors in data input and reference, check the integrity of database, check for consistency of data, check for uncertainties in data, database files, etc., undertake completeness checks, compare new results to previous results	All groups perform QA activities. The review of internal documentation and the check of methodological and data changes resulting in recalculations are not done.
20	Testing of the software tools	All groups are testing the tools. Test classes are used, manuals, GUI testing, with each test has its own code.
21	Testing done by a dedicated and independent person/group	In two groups testing is done by an independent person/group; in one group not
22	Written policies in place and employed for the test activities?	No written policies exist in all groups. Test documents are available, but no policies.
24	Risk-based testing? (Risk based testing uses risk to prioritize the appropriate test cases)	No risk-based testing is done.
25	Do you test according to risks of GCP relevance (e.g. risks for patient's wellbeing)?	In two groups GCP risk is considered; in one group not
29	Software Quality Control / Testing Plan	In two groups Quality Control / Testing Plan exists; in one group not. The plan covers unit tests / classes, GUI tests.
30	Is the testing done in a systematic way?	Testing is done in all groups in a systematic way
31	Separation of development, test and operational activities exist	This requirement was not understood. One group has implemented the separation partly.
33	**Test plan** covers the following points: system characterization, incl. status of development, objectives of testing/relationship to risk analysis, test cases, test data, including acceptance criteria, performance, amount of testing, results of tests, including descriptions of deviations, assessment of results, if applicable changes dependent on the development phase (SDLC) and repeated testing.	All groups have a kind of test plan that covers all topics. Though, no written, dedicated test plan document exists
34	Systematic approach to the specification of the amount of testing	No group has a systematic approach to specify the amount of testing
35	Evaluators/reviewers are different persons than the developers	In two groups this is not the case, in one group this is the case

38	Definition, from which change on a re-testing, completely or partly, is necessary	No group has a clear definition. Testing is always done when software is implemented
39	Definition of responsibilities for change management (release of change, implementer, reviewer)	In two groups the responsibilities are defined, in one group not. This covers that ticket is assigned, bug report created.

40	Are SOPs for using the tool (system) available and maintained?	User SOPs are in development in two groups, not in one group.
41	A security system maintained that prevents unauthorized access to the data?	All groups maintain a security system. This applies to the reference installation and depends on the final installation.
42	A list is maintained of the individuals who are authorized to make data changes	A list is maintained by one group, not by two groups.

43	Allows the tool **direct access** to source data/documents for trial-related monitoring, audits, IRB/IEC review, and regulatory inspection?	This requirement is difficult to understand. One group allows to access for source data, two not. Is the access to HIS data involved?
44	Requirements documentation (e.g. functional requirements) can be provided to support system validation	For two groups this is partly the case, for one fully.
45	Test documentation can be provided to support system validation	For two groups this is partly the case, for one fully.
46	Can test reports be provided to support system validation?	For two groups this is partly the case, for one fully.
47	Test reviews, including document reviews, performed in the different phases of tool development (IQ, OQ, PQ)	For two groups this is partly the case, for one not. This will be done when necessary.
48	Does the developer or another p-medicine group perform **system validation** of the developed software?	For two groups this is partly the case, for one fully
49	Do test reports exist that can become part of the validation plan?	For two groups this is partly the case, for one not
50	Access control policy exist	For two groups no access control policy exists, for one it exist. No written document exist; but a conventional basis.
51	User access management and user registration exist	Exists in all three groups
52	Does a policy for user password management exist?	Exists in all three groups; is freely definable

53	Decisions on the extent of validation and data integrity controls are based on a justified and documented risk assessment of the system	A documented risk assessment is done by none of the groups. Though, the extent of validation and data integrity controls can be justified.

54	Can close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT personal be shown?	Close cooperation exists in all three groups; but it cannot be demonstrated (e.g. document)
55	Is it assured that the competence and reliability of a supplier are key factors when selecting a product or service provider?	This is in one group the case. For example, external libraries for code, databases are used from external sources. The provider must be reliable.
56	Is it assured that quality system and audit information relating to suppliers or developers of software and implemented systems are being made available to inspectors on request?	This was seen as not relevant. No such policies exist. The system can be shown, processes can be demonstrated.
57	**Listing** of all relevant systems / components and their GXP functionality	A listing does exist in two groups, not in one group. There exist no written lists of GXP functionality.
58	Description for critical systems of the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures	A description exists for two groups, for one it is not relevant. The description exists in p-medicine deliverables documentation
59	User Requirements Specifications describe the required functions of the computerised system and are they based on a documented risk assessment of GXP impact.	URS exist in two groups as use cases in p-medicine, not in one group

60	Is the customised computerised system **formally** assessed and are quality and performance measures for all the life-cycle stages of the system reported?	None of the groups conducts a formal assessment; though assessments are done
61	Demonstration of evidence for appropriate test methods and test scenarios. Are system (process) parameter limits, data limits and error handling considered?	Evidence can be demonstrated in all three groups; though not for data limits and not 100% for everything else.
62	**Risk management** of the tools that cover the criticality and the potential consequences of erroneous or incorrectly entered data	Risk management is considered by no group. Though, correctness of data is tested (e.g. CRFs) and ObTiMA allows data checks. This is a problem of the implementation of CRFs and the creation of CRF.
63	Is data secured by both physical and electronic means against damage?	This is the case in one group, not in two groups. For test environment, this is problem of implementation. For the test environment of ObTiMA this feature is available.
64	Is stored data checked for accessibility, readability and accuracy? Can the access to data be ensured throughout the retention period?	Data is checked by all three groups. This is a problem of the implementation.
65	Regular back-ups of all relevant data	Regular back-ups are performed by two groups, not by one. This is a problem of the implementation.
66	Is the integrity and accuracy of back-up data and the ability to restore the data checked?	This is done by two groups, not by one. This is a problem of the implementation.

67	Obtain clear printed copies of electronically stored data	This is the case for all groups.
68	For records supporting batch release, is it possible to generate printouts indicating if any of the data has been changed since the original entry?	This is the case in no group. It is possible, but not yet implemented
69	Are audit trails available and convertible to a generally intelligible form and regularly reviewed?	This is possible for by two groups, not for one group. It is possible to implement.
70	Are any changes to a computerised system including system configurations only possible in a controlled manner in accordance with a defined procedure?	This is done for by two groups, not relevant for one group. This is a problem of the implementation.
71	Are computerised systems evaluated periodically to confirm that they remain in a valid state and are compliant with GXP? (Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports).	This is not relevant for developer group

72	Physical and/or logical controls are in place to restrict access to computerised system to only authorised persons	Controls are in place in all three groups. Though, this is a problem of the implementation.
73	Does the extent of security controls depend on the criticality of the computerised system?	This is the case in two groups, not relevant for one group. This is a problem of the implementation.
74	Are the creation, change, and cancellation of the access authorizations recorded?	This is the case in two groups, not relevant for one group. For ObTiMA this goes through the audit trail Server access is local
75	Are all **incidents**, not only system failures and data errors, reported and assessed?	Considered as not relevant by all groups.
76	Are electronic records signed electronically (e.g. password)?	This is possible for by one group, not for two groups. It is done indirectly during log-in with password.
77	Does the electronic signatures have the same impact as a hand-written signature; is it permanently linked to its record, and includes the time and date that it was applied?	This is not the case for two groups, and not relevant for one group. An audit trail is link to the record exist.
78	Is archived data checked for accessibility, readability and integrity?	Considered as not relevant by all groups. Server backup is daily. The proof of concept of the accessibility has been checked initially
79	If relevant changes are made to the system, is the ability to retrieve the data ensured and tested?	This is the case for all three groups. The proof of concept of the ability to retrieve the data has been checked initially.

4.2.1.3 Technical requirements for ObTiMA use for data collection in clinical trials

(Because questions could have several sub-questions, specifications, several answers per requirement are possible (e.g. y, y, n) n=no, y=yes, n/a= not applicable). Implemented=green, not implemented=red).

No	Requirement ObTiMA	Implementation
1	multiple studies at the same time	y
2	no limit to the number of studies	Theoretically, y
3	no limit to the number of patients	Theoretically, y
4	no number of users to use system	Theoretically, y
5	no limit to the number of **validity rules** that can be defined for a study?	y
6	No limit in the number of data fields	y
7	repeating data items	y
8	repeating forms,	y
9	repeating study events,	n
10	conditional forms	n, planned
11	data items visible under conditions	y
12	modification of eCRF after creation	Y
13	creation of eCRFs in different steps	n
14	eCRF with header for each form	
15	versioning of eCRFs	y
16	library with eCRF elements	Y
17	CRFs can be assigned to a visit.	n, planned
18	Sample collection assigned to a visit	n, planned
19	Repeating visits	n
20	Support of CDASH	n
21	CRFs for international trials	n, planned
22	Consideration of different time zones	n/a
23	Lab data shown in eCRF	n
24	no limit to the number of parameters in eCRF	y
25	no limit to the number of validity	Theoretically, y
26	use of different date formats	y
27	handling of incomplete date information	partly
28	Support of derived data items	n
29	change/update of eCRFs during study	y
30	different environments for data entry	y
31	integrated help functions	y, limited
32	consistency with a defined field type	y
33	uniform use of international units	n
34	supplementary functions for data monitoring (spell checking, conversion of parameters,…)	n, n, planned, no
35	different options for data input (saving incomplete eCRFs, error messages,..)	Y, n, y, partly
36	training for CRA, investigator, data manager and data entry personal	n
37	user support for forgotten pass words	y
38	help desk for users	n, partly

39	Offering of training for system administrators?	n, by STaRC
40	Training for monitors	n, by STaRC
41	Training for study managers	n, by STaRC
42	additional training	n, by STaRC
43	support / hotline services (hotline, English, Email hotline, training, …)	n, n, n, n, n, n, n, n, partly
44	documentation for training (manuals, video)	n, in preparation
45	support for eCRF design (preparation in collaboration, collection of sample eCRFs is available,…)	n, y, n
46	support for **installation** of software updates (technical support, automatic update, test scripts, …)	n, n, n
47	support for the expansion of software (new interfaces, new functionalities)	Y
48	services (support for error correction regular updates, user groups, …)	n, n, n planned
49	eCRFs can be tracked/depicted/searched by patient, site / investigator, visit …)	Y, n (planned), n, n, n, n
50	incomplete eCRFs are indicated by flags	y
51	Electronic signature for eCRF for approval	n
52	import of lab data into the eCRF	partly
53	laboratory reference ranges	partly (biobanking)
54	definition of ranges for each laboratory parameter	y
55	status for data items / forms / study events / subjects / query status	partly
56	display of graphic status icons	y
57	plausibility checks during data entry	y
58	plausibility checks in batch mode	n
59	**Audit Trail** records data input actions, data changes, date/time stamp …	y, y, n, y, y
60	Features of “Reason for Change” of audit trail	y, y, y, n, y
61	„Self Evident Corrections”	n
62	query system for data cleaning	n
63	Queries can be listed according to criteria (patient, site/investigator, country,…)	n
64	manual queries	n
65	queries can be “resolved”	n
66	Features of data query system	n
67	Identical queries are not generated	n
68	options for eCRF validity checks (mandatory fields, conditional branches)	Y, y, y, y, y
69	Are unresolved queries flagged?	n
70	investigator information about new queries	n
71	queries created by checking discrepancies	n
72	link between the query and its discrepancy	n
73	link of manually raised queries a data item	n
74	single step for correction of data item and query answer	n
75	query numbers	n

76	Printing of list of queries	n
77	transfer of a study subject with all data	y
78	data sharing with patient registers	n
79	lock and unlock a study (read only access)	n
80	input data from medical records	n, planned
81	sponsor does not have exclusive control over source documents and eCRF data	n, partly
82	copy of eCRFs stored independently from the study database at the site	n, partly
83	medical record for data collection	n, planned
84	notification system integrated	n, planned
85	options for management of patient study data (ID for study subject, anonymous / pseudonymous, …)	Y, y, y, y, n, n,
86	administration of eCRFs (date-/ time stamp, logging, verification code)	y, partly, n
87	status types of eCRFs	y
88	fully automatic status checking	y, y
89	planning of monitoring visits	n
90	source data verification (e.g. remote monitoring)	partly, n
91	randomization	n
92	interface randomization service	n
93	medical coding of terminology	n, planned
94	manage different coding releases	n
95	different language versions of the same coding dictionary	n
96	auto-coding	n
97	Recording of coding decisions	n
98	printing of “annotated CRFs”	n, partly
99	Printing of filled out/saved eCRFs	y, through export
100	Generation of reports	partly
101	filter reports by e.g. site, subject, form, …	n
102	import of study data	n, planned
103	import formats	y, (HIS data)
104	export of study data and metadata	y
105	filter data for export	y
106	CDISC certification	n
107	Reports for edit checks, derivations, integrity checks	n
108	Printing of report, acc. Visits, eCRFs items	n
109	Change Management of CRFs (with Version Control)	n
110	country-specific reports	n
111	types of analyses (e.g. recruitment lists, data quality)	n
112	configuration of analyses by centres, period, patient parameters, etc.	n
113	standard reports provided (interim reports, recruitment reports,…)	n
114	study related documents (eDocuments): patient identification, patient consent forms, specimen list)	n
115	management of eDocuments (date-time stamp, version control)	n
116	selection and access options for eDocuments	n
117	Support of many web browsers	Y, all
118	Is the data transfer encrypted?	y
119	Hosting of system	Y

120	well-defined and stable application interface (API),	y
121	extended data protection scheme	y
122	step-by-step database lock (e.g. soft lock) per patient, per site, per eCRF	partly
123	step-by-step database unlock per patient, per site, per eCRF	n
124	Any database lock or unlock is automatically recorded	y
125	report about locked data	Y
126	Export of complete study database	y, ODM
127	export only the eCRFs / collected study data per site	n
128	Is study archiving supported (database export, eCRFs export as PDF, references)	Y, y
129	information about system stability and system availability (e.g. load test / stress test) / performance test)	n, planned
130	trivial administration issues performed automatically (forgotten pass word)	partly
131	Password and log-in features cover minimal password length, forced password change, defined complexity, password history)	Mechanism is available, y, n, n, y, n, n, y
132	definition of user roles with specific rights	y
133	User Groups with specific rights	Y
134	Integrated safety procedures encrypted sending of usernames, encrypted saving and storage, backup-restore system, …	n, y, y, y, y, y
135	**Installation Guidance** including scripts	no, in development
136	installation by ECRIN data centre personal	Y
137	User manuals	no, in development
138	Support of system validation (providing validation documents (requirements, test results, QA documents), **test scripts)**	no, in development
139	**maintenance** of the system	n, not yet decided

The analysis shows that although many technical requirements to support GCP compliant data management in clinical trials are already met by ObTiMA, several requirements have to be still implemented, covering:

- CRF organisation (visits, internationalisation, input of lab values)
- Support and training for monitors, study managers; user manuals, updates and error correction as service
- Query system
- Loch/unlock of study database
- Randomisationservice
- Coding functionality
- Support of change management
- Reporting (e.g. recruitment rate, deviations)
- Links to study related documents

4.2.1.4 Technical requirements for Biomaterial Manager tool in clinical trials

(Following requirement domains are indicated in different colours in the middle column: study set-up; sample acquisition / check-in; selection/requests for samples/retrieval; management/interoperability; security/data protection. Several answers per requirement are possible, n=no, y=yes). Implemented=green, not implemented=red).

No	Requirement	implementation
26	Creation of users, centres, institutions	y
27	Biosampling is integrated with clinical data management	y
28	input of biosamples information in eCRF	y
29	Assignment of study centres (sites)	y
30	capture automatically the current date and time	y
31	unique identifiers (pseudonyms) for patients	y
32	Samples should be managed, employing centre details, analysis / extraction lists, addition of extraction, …	partly
33	controlling processes like audit trail, data history, notification list, list of assigned centres, …	y
34	set up of a new clinical study	y
35	System should be able to consider sites of a trial (leading investigator, study number, study start, sites, …)	y
36	Management of centres (sites): number of participating sites, patient recruitment, status, number of collected samples,…	y, partly
37	Management of central sample repository (CSR)	y, Obtima supports the creation of virtual biobanks
38	Set up of new institutions, labs or clinics	y
39	Each CSR can have assigned any number of study sites	y (virtual biobank)
40	institute set up: name of institute, type, responsible person	y
41	sample acquisition: upload and associate signed informed patient consent forms	n
42	link/reference to the patient informed consent	partly
42	creation of informed patient consent form templates (understandable language, research projects, future use of the samples)	n
44	withdrawal of patient consent by the patient	n
45	alteration of scope of patient consents	n
46	enter new biological sample records	y

47	in addition to compulsory sample data, the system should allow users to enter the following data (identifier, depositor's name and address, source, substrate, …)	y
	storage of shipping records (shipping log)	n
48	anonymization of samples by removal of identifying data and by two-way coding	Not applicable
49	review of the anonymization	Not applicable
50	anonymization and review must be logged	Not applicable
	generation of a pseudonym for a barcode (BC1)	y
51	second pseudonym for a second barcode (BC2)	n
52	check-in of patients, including following information: informed consent is available, BC1, BC1 and BC2 checked for validity, …	partly
53	creation of a new trial; with pseudonymisation of barcode 1, BC1+2 is checked for validity	partly
	It should be possible to check-in patients	Yes
54	system must guarantee that samples of studies are coded threefold: Study participant number, first pseudonym (BC1), second pseudonym (BC2)	no
55	BC2 replaces BC1	no
56	unequivocal patient number (IC)	y
	check-in of patients without IC entry should be possible	y
57	identification only by BC2 (second pseudonym)	n
58	inventory list of all samples collected for a study, per site or patient	n
59	no limit on the number of BC codes possible	n
	system should be able to read BCs	y
60	possible that a patients withdraws from a study, inclusive the deletion of patient number / sample	n
61	system should allow the change of centres	partly
62	check that BC2 has been assigned to a sample before the sample is being stores in the biobank	n
	check of validity of the informed consent	n
63	request informed consent information	n
64	check that all patients of a study have been assigned to a site	y
65	pseudonymisation of patient's informed consent	y
	guarantee that assigned BC is not used again in the study	y
66	BC1 verification	n
67	patient identification number (study-ID)	y
68	double input of patient study numbers	n
	tracking of physical location of samples	y
69	tracking the movement of samples by recording: current location, previous locations, date of movement	n
70	validation of samples by recording: location of validation, list of items validated, date of receipt of items to validate, date of validation	n

	request and selection of samples	y
71	Upon request a list is generated: study, CSR, number of samples, due date	n
72	list is generated covering all samples of the request (SGN, BC2, material, amount,…)	n
73	list with selected BC2s is send to the sample manager	n
74	request of sample status: destruction requested, destroyed, lost, shipped	n
	Request for sample selection	y
75	A trustee should be able to search for patients	y
76	sample retrieval recording: date of request, list of samples requested, person who requested samples	n
77	approve, partially approve or reject sample requests	n
78	interface with a biobank management system	n
79	creation of new users	y
80	administrator can assign following roles: data manager, process controller, auditor, Lab administrator, sample registrar, sample manager	y
81	list of all users	y
82	trustee can make changes in the system concerning the informed consent of patient	n
83	process controller and auditor can see all processes in the system	n
84	export of sample records, a catalogue of samples	n
85	logging of all export operations.	y
86	Import of sample records, records of other entity types	y
87	open or a well-document proprietary data interchange format	y
88	graphical user interface.	y
89	display of text elements in the local language	y
90	Documentation of functions, fields in data entry forms, errors and possible solutions	n
91	online help	n
92	Assistance during data entry (drop down menus, default values)	y
93	error messages or alerts	y
94	error messages must be meaningful	y
95	system recovery	y
96	automatic backup feature	y
97	recovery feature for restoring entities	y
98	data backup must be checked regularly	y
99	recording per log: action, entities involved, user, date,…	y
100	recording automatically of critical actions: actions which result in deletion of entities, data modifications, access violation,…	y

101	Forbid access without authentication	y
102	authentication by user ID and password	y
103	data during authentication cannot be intercepted	y
104	logging of successful and unsuccessful authentications	y
105	not reveal information about validity of user ID	y
106	refusal to accept further attempts from one address	y
107	Forbid unsecure passwords	y
108	adherence to privacy laws for information systems.	y
109	withdrawal of consent is clearly defined and conveyed	y
110	Anonymization is verified by review procedure	y
111	management of information: sample acquisition, storage of samples, processing of samples, disposition, selection, retrieval of samples	partly
112	No association of identifying data with non-identifiable samples	y
113	encrypted storage of passwords.	y
114	encrypted storage of protected health information and personal data	y
115	testing if input value matches the defined format	y
116	input value satisfies metadata constraints (e.g. age)	y
117	check of spelling in text field inputs	n
118	authorized users access: sample records, procedure records, documents (e.g. informed consent), user records	y

The Biomaterial Manager is integrated into ObTiMA. Sample specifics can be input into a special CRF form. This tool fulfils nearly all technical requirements. Requirements that have still to be implemented cover the handling and checking of informed consents during sample acquisition, a two step pseudonymisation (may not be necessary and depends on the privacy framework of p-medicine), the verification of bar code and pseudonymisation, the validation of samples, reporting about samples (e.g. retrieval), online help.

4.2.1.5 Technical requirements for imaging support in clinical trials

(Following requirement domains are indicated in different colours in the middle column: general aspects (limitations); quality aspects of imaging; process aspects; data security/data protection; training and support; platform requirements. Several answers per requirement are possible, n=no, y=yes). Implemented=green, not implemented=red).

No	Requirements for imaging (Dr.Eye)	Implementation
1	image handling during clinical trials	y
2	image handling during multiple trials at the same time	y
3	no limit to the number of trials	y
4	no limit to the number of images	y
5	no limit to the number of users	Not applicable
6	no limit in the size of the images	y
7	components of your imaging system: PACS, connection to CDMS, DICOM viewer, image processing unit	Yes, yes, yes, no, no, yes
8	system interacts with PACS	n
9	quality checks of incoming images	y
10	validated standardized image analysis techniques	y
11	standardized extraction of quantitative image information	y
12	validated and standardized image processing techniques	y
13	tool marked as a medical product (CE certificate)	n
14	loss-less transfer of information (imaging data)	y
15	Generation of transfer protocols	y
16	centralized analysis of imaging data	n
17	validated DICOM protocols for transfer of images	y
18	upload of image data accompanied by a quality check	No, in development
19	definition of generic quality specifications (Base Clinical, Clinical CT,...)	No, in development
20	measures performed on image bitmap (burned-in identifying information, evaluating of contrast, ...)	y
21	transmission of imaging data between sites and a central repository	No, could be implemented
22	combined management of imaging and numerical and other data by linking	No, could be implemented
23	high availability (site independent) and access to data, images and trial results	y
24	rules to be set up for individual studies (consistent use of DICOM tags,...)	No, could be implemented
25	visibility if a predefined condition is met	y
26	numerical analysis results exported into a CRF	n
27	input clinical trials images / clinical imaging data	n

28	send/receive images by the investigator from personal computer	No, in development
29	exchange with data management system for clinical trials (e.g. import image number in CRF, link between CRF and image)	n
30	central image repository for the clinical trial, local image repositories	Yes (PACS), Yes
31	transfer, up-/down-load and viewing of imaging data by local PC to/from PACS	No, in development
32	send/receive images by the investigator from the local PACS	No, in development
33	definition of study protocol parameter in tool to support the workflow	n
34	clean data / correct / edit data; audit trail	Yes, No
35	image post-processing and analysis	y
36	joint usage of CDMS/EDC, PACS and image processing tools	n
37	search in the imaging data bases	No, in development
38	reporting of forms related to image acquisition and analysis (e.g. presence of image artefacts or patient compliance)	n
39	DICOM and DICOM protocols	y
40	analysis results are sent back to the PACS (DICOM and DICOM Structured Reports)	No, in development
41	image analysis results are queried and retrieved	n
42	call PACS and the image processing unit from the clinical data management system for cross-linking of data and semantic searche	n
43	different environments: development, testing, validation, training, production / operation	No, in development
44	imaging data provided with expert annotations	y
45	managing metadata by tool	y
46	images tracked/depicted/searched for: patient / PID, site, visit / time, investigator,…	y
47	corrupted images are flagged	n
48	imaging review, with image approval functions	n
49	Assignment of status to images (e.g. image reviewed, image analysed)	n
50	handling of different types of images (e.g. MRI, CT, PET,…)	y
51	integration of a third party for image evaluation / review	n
52	analysis core lab can log in, submit, and retrieve data / images	n
53	standards supported (Integrating the Healthcare Enterprise (IHE), DICOM, HL7, and XDS	y
54	image retention (with policies, security policies)	n
55	generation of automated alerts (outliers, according to specified criteria,…)	n

56	long-term archiving of study images after the end of the study	No, in development
57	Source Data Management supported, eSDI requirements applied to imaging	n
58	controlled access to the data base / imaging repository (user account)	y
59	privileges and access rights controlled via user accounts	n
60	data security and privacy is guaranteed (different national laws are considered)	n
61	security relevant methods: https, eligibility check of users, image up-load leads to removal of private header information, generation of pseudonyms, storage data/images pseudo-anonymously, …	No, in development
62	tracking of image generation, transfer and storage	n
63	access rights for access to PACS	y
64	deny registration under specific conditions	n
65	support and training for CRA, investigator, image reviewer,…	y
66	user support for forgotten passwords	y
67	help desk for users	y
68	integrated help functions	n
69	Can you offer training for system administrators?	y
70	support and / or hotline services: hotline languages, telephone hotline, Email hotline, training by consultant,…	N, n, y, n
71	documentation for training (manuals, video, online documentation)	Y, y, y
72	parameterisation of your tool / image analysis validation: collaboration, training	N, Y
73	installation of software updates (technical support, installation Guidance including scripts, automatic update audit trail for upgrades test scripts, manual for updates)	Y, n, n, n, y
74	expansion of the software (new interfaces, new functionalities, new analysis algorithms,…)	partly
75	User manuals / SOPs are provided for data managers, investigators, image reviewers, image analysts,…	partly
76	system validation of the imaging system in ECRIN centre	If needed
77	support of installation of imaging system in ECRIN centre	If needed
78	support, by: providing validation documents (requirements, test results, QA documents), test scripts, image validation scripts	If needed
79	web browsers	Not applicable
80	encryption of image data transfer	Not applicable
81	well-defined and stable application interface (API)	n
82	Password and log-in features: minimal password length, forced password change, recording of password history,…	Partly
83	procedures integrated into the software: encrypted sending of usernames and passwords , backup-restore system, loss of connection triggers log-off,..	Y, n, n, n, n

The requirements for imaging in clinical trials are to some degree fulfilled in Dr.Eye. In must be considered that Dr.Eye does not support the entire imaging process but only the part of analysis and amendment. Requirements that have to be implemented by the p-medicine imaging tools must cover additional quality checks, ability to link imaging data with other data, easier way to implement study processes, transfer of images, link with data management system, integration of image analysis results, easy support for image reviews, generation of alerts, better inclusion of data privacy and security.

4.2.2 Software as a medical device

During the assessment of Dr.Eye concerns were stated to clarify when a software solution is considered as a medical device. The problem has been discussed in chapter 9.1.4 of Del9.1[53]. According to EU Directive 2007/47/EC[54] "medical device" means any instrument, apparatus, appliance, **software**, material or other article, whether used alone or in combination, together with any accessories including the **software** intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes. Software when specifically intended by the developer to be used for one or more of the medical purposes set out in the definition of a medical device has to be considered a medical device. Under following conditions, software has to be treated as medical device[55]:

- Software is used for diagnosis, monitoring or treatment decisions
- Purpose of the software is to control or influence the functioning of a medical device (as specified by EU Directives)
- Software is used for the analysis of patient data generated by a medical device, with a view towards diagnosis and monitoring
- Software is designed to be used for, or by, patients in the diagnosis or treatment

For example, a PACS used for administrative purposes may not fall under the definition of a medical device if only intended for archiving and storage of data, without any manipulation of the images. But a PACS used for viewing, archiving and transmitting images is generally classified as Class I medical device. Furthermore, a PACS containing functions for post-processing of images for diagnosis (image processing, complex quantitative analysis, image enhancing functions) has to be classified under Class IIa or IIb. In this context, it may be that the amendment of images by Dr.Eye can be seen as a processing of the image that result in an enhancement that has a direct impact on the diagnosis and treatment of the patient. Considering this classification, Dr.Eye and perhaps other tools in p-medicine should be assessed if they have to be validated as medical devices. Even it is not the aim of the p-medicine project to develop commercial software and services it should be necessary to ensure sustainability of tool provision to fulfilling all regulatory requirements, including the medical device law.

[53] Del9.1: Report of regulatory and international aspects of the clinical trials. p-medicine (01.02.2012).

[54] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:247:0021:0055:en:PDF

[55] Klümper M, Vollebregt E.: Navigating the New EU Rules for Medical Device Software.RAJ Devices Mar/Apr 2009, 83-88 (2009)

4.2.2.1 Results of quality management and GCP assessment: for the development of recommendations

Area	#	Criteria	Status	Evaluation	Observation
Development Practice	1	SOPs or equivalents exist covering development procedures, roles, responsibilities etc.	mandatory	-	No SOP or equivalents for Development are in place. This bears the risk that development is performed without considering GCP or other quality measures. Risk that new developers do not develop considering patient safety, GCP and do on.
	2	SOPs or equivalents exist covering software change and configuration management	mandatory	-	SOPs or equivalents covering software change and configuration management are not available. This bears the risk that changes are performed without considering GCP, resource/cost implications or other quality measures. Further this bears the risk that changes are performed without assessing the risks for patient's safety.
	3	A development plan is being used for the system(s) currently in development, in line with stated policies and methodologies	mandatory	+	
	4	Functional specification documents available and used as part of the development process	mandatory	+	Requirement Specification still in development, an agile deveploment model is used.
	5	SOPs or equivalents covering testing, continuous integration (CI), sign off / deplyment procedures etc.	mandatory	o	CI, Testing performed. No exisiting test plan or policies.
	6	Modern source control implemented (e.g. Git, Subversion, Mercurial)	mandatory	+	
	7	Unit testing used and integrated with development and CI	mandatory	+	
	8	Integration testing used and integrated with development and CI	optional	o	
	9	There is evidence of peer review / support amongst developers	optional	-	Internal peer training.
	10	System has been stress tested under high data load	optional	-	
Validation	11	Functional specification documents are available to users to support validation in their own environment.	mandatory	+	
	12	Validation scripts are avalable to users to support validation in their own environment	optional	-	Validation scripts are not available.
Non-Functional Aspects	13	Managing and ensuring security is part of the functional specification and / or development plan (e.g. anti-SQL injection)	mandatory	o	partly fulfilled
	14	Error handling / logging / reporting part of the functional specification and / or development plan (but not optional!)	mandatory	o	partly fulfilled
	15	Access control aspects part of the functional specification and / or development plan (e.g. authentication and authorisation mechanisms)	mandatory	+	
	16	System should record the access control authorisations managed within it	mandatory	-	not available
	17	System allows selected data to be stored encrypted	optional	-	?
Regulatory compliance	18	The system can support audit trails for data as defined by GCP	mandatory	+	
	19	The system can display, report data and audit data in forms that support inspection and audit	mandatory	o	Not available
	20	The system can support recording of source data verification	optional	-	not available
	21	The system can support blinding of intervention type when necessary	optional	-	not available
	22	The system can support pseudonymisation of data	optional	-	not available
	23	The system can support electronic signatures if necessary	optional	+	

User Support	24	Training courses are available to users	mandatory	-	Not available
	25	Training materials and system documentation is available to users	mandatory	+	
	26	A test / demo installation is accessible	optional	o	?
	27	Help desk / response facilities can be arranged	mandatory	+	
	28	Technical documentation is available to users	mandatory	+	
	29	Technical support arrangements are available	mandatory	+	
	30	Installation specification and documentation is available to users	mandatory	+	
	31	On-site Installation support is available	optional	+	
Ongoing Development	32	System providers have a commitment to / capability for ongoing bug fixes	mandatory	-	not available
	33	System providers have a commitment to / capability for ongoing development	mandatory	-	not available
	34	Functional specification of updates will be made available	mandatory	-	In order to validate and evaluate the software is it essential that a complete functional specification is provided for end users.
	35	Test scripts will be made available for updates	optional	-	not available
	36	System should include mechanisms for reporting bugs and making feature requests	optional	+	

4.2.2.2 Evaluation criteria classification: ObTiMA

Evalution Criteria Classification	Priority	Criteria	Evaluation
QA	Mandatory	Software change and configuration management	y (feature request hs writtwn policy)
		Information Security Policy	y
		Development Plan (SDP)	y
		Quality Measures or Assessment	y
		Developer Training/Education	n (peer training internally)
		Requirements management, or requirements engineering	y, no review by management
		Quality Policies	y
		Test policies	n
		Quality Management Plan	y
		Testing Procedures	y, no test plan
		Regulatory Compliance	y
	Optional	SOPs for Development	n (good practices are used)
		Programming Standards	y
		Technical Documentation	y
		Version Control	y
		Audits, Reviews and Supervision	n
		Naming Conventions	y
		Error Handling	y
		Conventions for UI	y
		Conventions for Platform	y
		Code Review	y
		Standards of Documentation	n, no doc review
GCP-Compliance	Mandatory	Accurate Reporting and Interpretation of Clinical Trial Information	y
		Confidentiality and Privacy of subjects protected	y
		Accuracy, Eligibility, Completeness and Timeliness of data	y
		Evaluation of patient risks during development	y
		Source Data Verification	y
		Audit Trail	y
		Blinding of Data	y (identity blinded)
		Pseudonymisation	y
		Link of electronic signature with date and timestamp	no signature
		Audit, Monitoring and Inspection Capabilities	n
Computerized Systems Validation (Annex 11)	Optional	Support IQ, OQ and PQ	y, can be done as service
		Support Systems Validation	partly
	Mandatory	Staff Training	n
		Written Policies Developer Audit	n
		Testing GCP-Compliance	y
		Requirements Documentation incl. GCP Impact	y/n URS exist as use cases
		Testing Documentation	y, test cases, test data, no test plan
		Test Reports	y
		Risk Assessment of used standards, protocols, procedures and records	y
		Risk Assessment of Errors and incorrect Data	partly
		Printed Copies of electronically stored data	y
		Regular Review of Audit Trails	
		Test of stored data (accuracy, accessibilty and readibility)	as proof of concept intitially done

Security	Optional	Access Control to source code	y
		Control of technical vulnerabilties	y
		Access Control Audit Trail	y
	Mandatory	Data Change List of Individuals	y
		Protection against malicious and mobile code	y
		Access Control Policy	y
		Policies for User Password Management	y
		Secure Logon prcedures	y
		User Authentication & Authorisation	y
		Cryptographic Control	y
		Secure Entry and Processing of data	y
		Physical and electronic Security	y
Training	Optional	Training Courses (Video, Webinar, Webpage)	can be prepared
		Demo Installation or Demo	y
	Mandatory	Training documentation	n
		Training Policies	n
		User Training	n, can be done
Support	Optional	Help Desk (Telephone, Email, Webbased)	not yet, assignement of stuff necessary
		User Group	depends on business plan
		Testbed Installation	y, reference installation
		Systems Documentation	partly, technical docs
		Installation Guide	in development
		Installation Assistence	can be provided
	Mandatory	User Support	depends on business plan
		Change Management	y, ticket system
		User Documentation	in development
		Technical Support	depends on business plan
		Support for Error Corrections (Bugfixing)	y
Maintenance	Optional	Upgrade or Update Support	depends on business plan
		Audit Trail of Updates	n
		Test Scripts for Update	n
	Mandatory	Provision of Upgrades, Updates and Patches	depends on business plan
		System Recovery and Backup Strategies	y
		Restore of data	y
Availability	Optional	SLA	
	Mandatory	Emergency and Rescue Plan	n
Stability	Optional	Load Test, Stress Test, Performance Test	planned

4.2.2.3 Evaluation criteria classification: Dr.Eye

Area	#	Criteria	Status	Evaluation	Observation
Development Practice	1	SOPs or equivalents exist covering development procedures, roles, responsibilities etc.	mandatory	+	
	2	SOPs or equivalents exist covering software change and configuration management	mandatory	o	SOPs or equivalents covering software change and configuration management are not available. This bears the risk that changes are performed without considering GCP, resource/cost implications or other quality measures. Further this bears the risk that changes are performed without assessing the risks for patient's safety.
	3	A development plan is being used for the system(s) currently in development, in line with stated policies and methodologies	mandatory	+	
	4	Functional specification documents available and used as part of the development process	mandatory	+	
	5	SOPs or equivalents covering testing, continuous integration (CI), sign off / deployment procedures etc.	mandatory	o	CI, Testing performed. No exisiting test plan or policies.
	6	Modern source control implemented (e.g. Git, Subversion, Mercurial)	mandatory	+	
	7	Unit testing used and integrated with development and CI	mandatory	+	
	8	Integration testing used and integrated with development and CI	optional	+	
	9	There is evidence of peer review / support amongst developers	optional	o	partly fulfilled
	10	System has been stress tested under high data load	optional	+	

Security	Optional	Access Control to source code	n
		Control of technical vulnerabilties	n
		Access Control Audit Trail	not relevant
	Mandatory	Data Change List of Individuals	n
		Protection against malicious and mobile code	?
		Access Control Policy	y
		Policies for User Password Management	y
		Secure Logon prcedures	y
		User Authentication & Authorisation	y
		Cryptographic Control	not relevant
		Secure Entry and Processing of data	not relevant
		Physical and electronic Security	not relevant
Training	Optional	Training Courses (Video, Webinar, Webpage)	manuals
		Demo Installation or Demo	?
	Mandatory	Training documentation	manuals
		Training Policies	n
		User Training	y
Support	Optional	Help Desk (Telephone, Email, Webbased)	y, Email
		User Group	y, administrators
		Testbed Installation	n
		Systems Documentation	y
		Installation Guide	Technical support & manual
		Installation Assistence	Technical support & manual
	Mandatory	User Support	Technical support & manual
		Change Management	n
		User Documentation	y
		Technical Support	y
		Support for Error Corrections (Bugfixing)	y
Maintenance	Optional	Upgrade or Update Support	n
		Audit Trail of Updates	n
		Test Scripts for Update	Technical support & manual
	Mandatory	Provision of Upgrades, Updates and Patches	Technical support & manual
		System Recovery and Backup Strategies	not relevant
		Restore of data	not relevant
Availability	Optional	SLA	
	Mandatory	Emergency and Rescue Plan	n
Stability	Optional	Load Test, Stress Test, Performance Test	performance tests

4.2.2.4 Summary of the results of the survey about quality management and development process control

A heatmap (Fig. 6) gives an overview over the situation of quality management and process control at three developer sites. Still lacking at all three locations are (indicated red in Fig. 6) to a large degree: written policies, that SQA activities are independently and constantly reviewed, that documents are reviewed, SOPs for development activities and an information security policy.

No	Requirement	area	Dev.1	Dev.2	Dev.3
1	Is a conventional or agile approach used for software development?	SW development planning			
2	software development plan	SW development planning			
3	participate in training	SW development planning			
4	members are trained	SW development planning			
5	SOPs for the development activities	SW development planning			
6	an information security policy (ICP)	SW development planning			
7	Information security awareness	SW development planning			
8	memknowledge / experience with testing and validation bers are trained	SW development planning			
9	previous audits or inspections	SW development planning			
10	familiarity with regulatory background for software for clinical research	SW development planning			
11	development according to SDLC	SW development planning			
12	development standards	SW development planning			
13	written policies for document review	SW development planning			
14	definition of documents review	SW development planning			
15	review process	SW development planning			
16	processes for deviations	SW development planning			
17	system documentation that covers system architecture	SW development planning			
18	Reference installations for separate phases	SW development planning			
19	written policies for integrity tests, security checks	SW development planning			
20	written policies for emergency precautions	SW development planning			
21	Software Quality Assurance (SQA)	SW development planning			
22	Review of Software Quality Assurance (SQA) activities	SW development planning			
23	quality assurance activities trained	SW development planning			
24	SQA review of the activities	SW development planning			
25	Written policy for managing requirements	SW development planning			
26	Written policy for managing	SW development planning			
27	Written policy for software configuration	SW development planning			
28	Written policy for employing software development process	SW development planning			
29	Written policy for training	SW development planning			

Fig 6: Heatmap of the results of the evaluation of quality management / process control at three developer locations (Dev1-3). Red=no implementation, green=implemented and used, yellow=partly implemented.

4.3 Risk based development and evaluation of p-medicine tools

For system validation, GAMP[56] recommends a risk based approach for a configurable software product (Fig. 7). There are two reasons ECRIN requires a risk based approach to quality management and system validation: increased efficiency and higher quality. It is possible to decrease the efforts for computer system validation and its costs by implementing a risk-based approach. Several guidelines recommend an integration of software life cycle management and risk management activities. Based on the intended use and the safety risk associated with the software to be developed, developers should determine the specific approach, the combination of techniques to be used, and the level of testing to be applied[57].

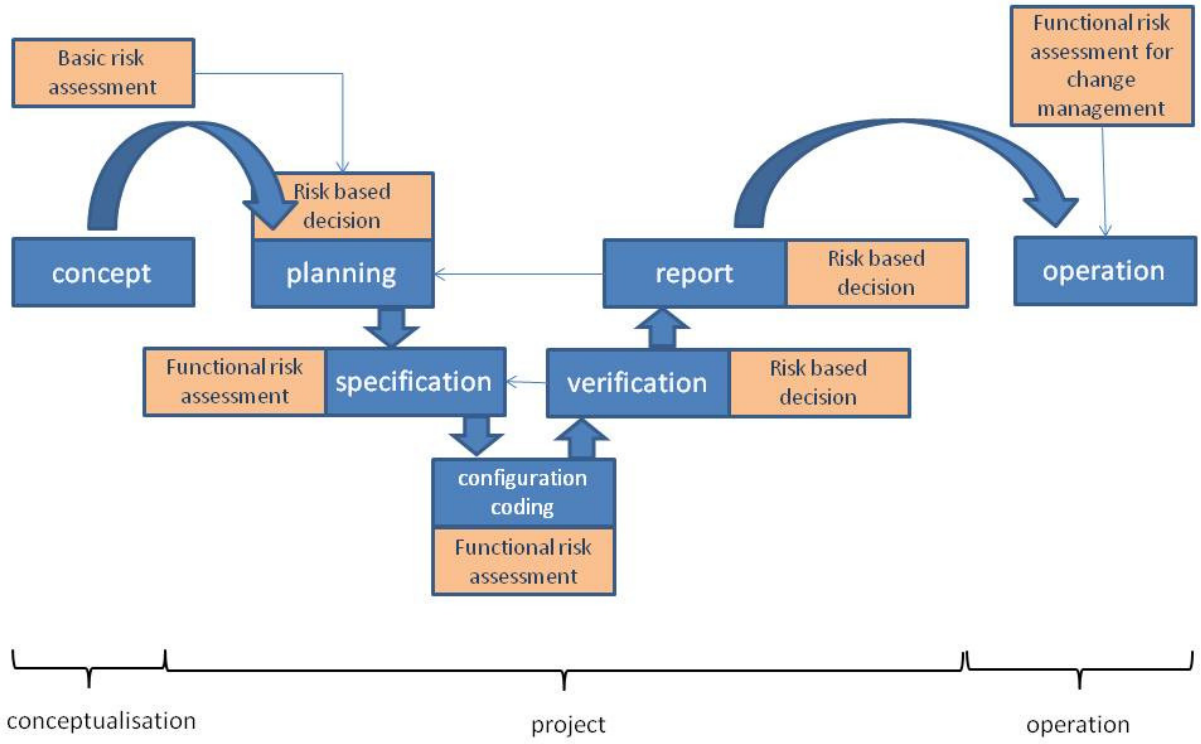


Fig 7: Different types of risk management should accompany the software development life cycle (SDLC). Especially important are the steps (curved arrow) from concept to planning and from validation report to operational system (modified from GAMP5).

There are additional, inevitable costs associated with the validation of the software system. If validation is not carried out correctly, it may cost as much or more than the price of the software itself[58]. The time required to validate software systems and the necessary resources are also often seens as problematic. The user can rely on a software company / software developer for help during validation, the less resources the user has to devote to validation. But to utilize developer documentation for validation purposes the user must first audit the vendor's test records prior to accepting any documents, results or data. Without a thorough understanding of the vendor's methodology and testing the user will not be able to defend

[56] GAMP5, idem

[57] FDA: General Principles of Software Validation; Final Guidance for Industry and FDA Staff. (2002).

[58] Ade D.: Advantages to Risk-Based Validation. GXP Lifeline Feature Article. MasterControl (2000).

the acceptance of the validation data of the developer. In case the developer's data is successfully assessed and audited, it can justifiably be accepted and be of benefit in reducing the cost and time required to validate the software system.

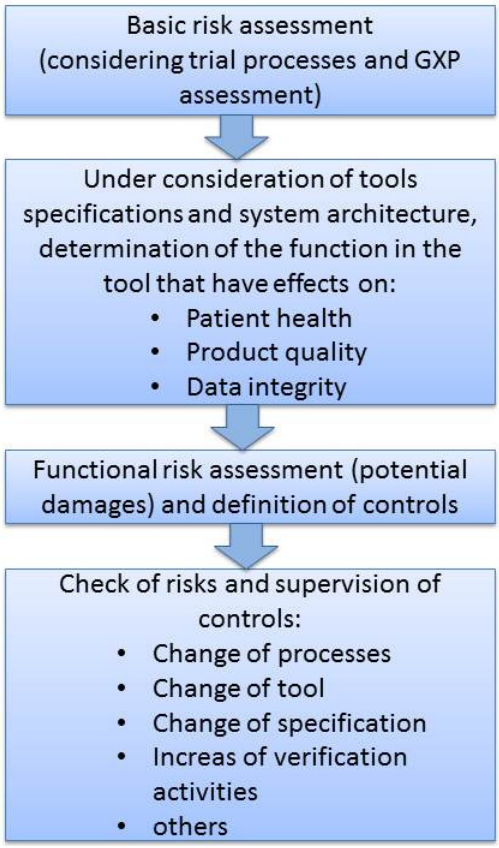


Fig 7: Hierarchy of risk assessments according to GAMP: basic risk assessment during software design phase, GCP focused risk assessment, functional risk assessment and during operations of the tool the check of risk and supervision of controls

A common attribute of successful risk-based validation is that the user is able to focus more on PQ testing and less on IQ and OQ testing. By using assessed and audited documentation from a developer the end result for ECRIN should be less validation work, faster system deployment in clinical trials and less validation costs. According to GAMP for system validation a risk hierarchie (Fig. 7) should be used that covers a basic risk assessment during software design phase, GCP focused risk assessment during IQ, OQ and PQ (see Fig. 8), functional riskassessment and the checking of risks during the operation phase of the tool.
Our assessment of the p-medicine developer groups showed that no risk based testing, no documented risk assessment and no specification of the required amount and the depth of testing exist. A more prominent role of risk management must be established in p-medicine.
As an introduction to risk management for p-medicine tools, an overview over the functional risks for three tools (Portal, OA, and ObTiMA) was developed (chapter 4.3.1) and a template for GCP focused risk is provided.

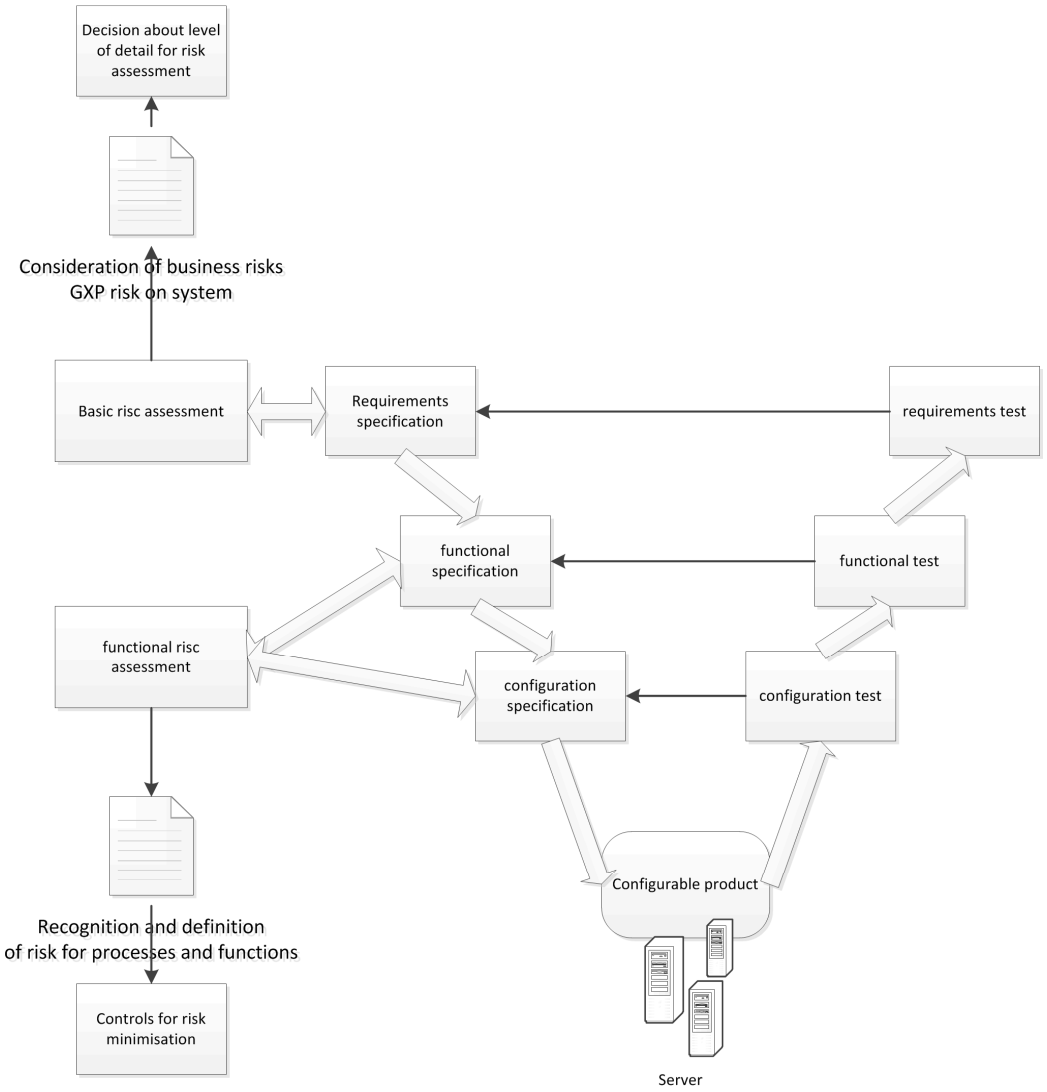


Fig 8: Risk based approach for a configurable software product as used by GAMP5[59]

4.3.1 Risk Assessment

Risk assessment is an important step in development of a software tool, as it enables the developers to be aware of potential problems ahead of time. When a risk is identified during the assessment, a solution and a contingency plan is also developed. Basic steps of a risk assessment are; identify, estimate the impact, have a mitigation plan and a contingency plan in case the risk occurs. According to GAMP the development process should be accompanied by different kinds of risk analysis. A basic risk assessment is done already at the conception phase to enable risk based decisions for the planning of the tool development (Fig. 8) and therefore are important for developers.

4.3.1.1 p-medicine PORTAL:

As p-medicine's portal will be the gateway through which users (clinicians and patients) will be accessing p-medicine, its risk analysis was a high priority. Though the risks of the portal in

[59] GAMP5 idem

general do not harm clinical data, they can leave the user inaccessible to the data stored in p-medicine and also to its tools.
Table (Appendix 7.1.3) summarizes the risks identified by the portal developers and their possible mitigation and contingency plans. Four risks with medium probability were identified which had high impact on the Portal itself and on p-medicine in general. Two of these risks relate to the possible crash of the Portal server, either due to hardware problems or inability of the server to restart automatically. For hardware issues, a possible mitigation solution is to have a ready for usage backup server. While the other two risks are related to issues of user sign into the Portal and can be prevented by regular checks and coordinating with other tools where access is restricted and user based.
The result of the extended survey covering also GCP compliance for the portal (Chapter 7.5.7.2) showed that GCP compliance criteria have been taken care of by the developers of p-medicine tools before integrating it into the Portal. The Portal itself does not store any clinical/patient data except of login information. As a contingency plan, before integration of the tool in the portal, the portal administrator should clarify with the developers of the tool if the corresponding is GCP compliant. A decision about an integration of a tool should be discussed with project leader. Portal developers identified one high risk for system security which relates to p-medicine's inability to continue support for critical processes like data entry.The mitigation plan in this case will be to use the backup server and requests the users to enter data again. Backup of the portal database and directories with important data (configurations, settings, workflows for data mining tool) as well as files for deployment of p-medicine tools is also available on the project server in IBMT. As a contingency plan backups should be made more frequently so that in case the recent back up fails, data loss is minimized

4.3.1.2 Ontology Annotator (OA):

OA is the p-medicine tool which allows data administrators to integrate and annotate data from different sources (genomic data, clinical data, image repositories etc) and import it into p-medicine. OA is used by expert users but its availability and risks could have a high impact on patient data and use of p-medicine by clinicans and patients alike.
Table (Appendix 7.1.4) summarizes the risks identified by the developers of OA. Of the six risks assessed, only one has a high impact on p-medicine while five have a high impact on OA itself. The risks with highest probability are server crashes (server which hosts either OA or the internal database). As a mitigation plan is in place (secondary server) this high risk scenario has a preventive measure in place. The risk with the highest impact on p-medicine, is if the page storing HDOT (Health Data Ontology Trunk) is unaccessible. A mitigation plan for this risk is also in place, where OA maintains a local copy of the HDOT files. The OA can work with the local copy, if this risk occurs.

4.3.1.3 ObTiMA:

Obtima is the tool used by p-medicine to allow its users (clinicians and trial administrators) to design, manage and collect patient data for clinical trials. As OBTIMA is the tool for data entry and storage ,risks pertaining to OBTIMA could have a high impact on clinical trial data and it has to follow strict GCP guidelines.
Table (Appendix 7.1.2) summarizes the risks OBTIMA's developers have identified. In all, these risks have a high impact on OBTIMA but retain a low level impact on p-medicine. Most of the risks assessed are related to the hosting server and improper access to the clinical data stored on the server. In case of server crash (hardware, software), the contingency plan is to first try to repair the problem and if not possible then import data from the backup server. For security risks, it is vital to house the servers in a locked, low access room and keep all data encrypted. In risk situations where unauthorized access is given, a mitigation plan is that access controls should have mechanisms, e.g. using roles, group membership, etc., that can be used to effectively differentiate and manage access.

4.4 Results of the gap analysis

4.4.1 Motivation of the gap analysis

Regardless of the motivation within the p-medicine project the same goals must be achieved for all components of the overall infrastructure to ensure that developed tools and services can be used within a clinical trial infrastructure:
Ensure that the system is compliant with the required standards, rules, and regulations and that it will be ensured over the lifetime of the software;
Controlled documents of implementation and maintenance activities show evidence that the system complies with the required standards, rules, and regulations.
Otherwise there will be doubts about the validity of the system, and those doubts will increase over time. The primary benefit for p-medicine is obviously compliance with regulations and avoidance of regulatory intervention. Such intervention can result in large fines, costly delays and expensive recalls. Moreover p-medicine will deal with patient's safety, so ensuring the compliance is not optional key factor or an added value, it ensures that the data of a patient is processed by considering following main requirements, such as:
accuracy, eligibility, completeness and timeliness of data
confidentiality and privacy of subjects is protected and
an evaluation of patient risks during development.
As part of the project p-medicine aims to bring new products to market. Part of the business should maintain and if possible improve the quality of the products and more important the business model shall sustain compliance with changing legislations, rules and regulations.
There are two principal motivations to validate computer systems:

- "Process validation (including computer systems) is required by Industry Regulators such as the FDA, MCA, and the EU. For example, the FDA Quality System regulation regarding Medical Devices[60] states that "when computers or automated data processing systems are used as part of production or the quality system, the manufacturer shall validate computer systems for its intended use according to an established protocol." Non-validated computer systems that are used in critical processes may lead to severe regulatory actions (including fines and product withdrawals) and higher maintenance costs, and thereby have a big impact on your business.
- Achieving High Quality standards and using those standards to support the validation effort. Through the validation of a system and the implicit requirement to use a QMS from the beginning of a project and throughout the life of a system, an organisation can reduce or eliminate the risks presented by their computer systems. Used in this way CSV can result in systems that are fit for purpose, satisfy users, are easy to support and maintain, and suffer less downtime."[61]

4.4.2 Results/Observations of the Evaluation / Gaps identified

The development of the tools is driven by a community with a high visibility of strong domain expertise. But as expected for an academic project, major findings were identified in the gap analysis that might delay or in worse case prevent the usage in a clinical trial infrastructure.
In summary following observations were made based on the self-assessment by tool or service providers:

- Business plan/model is still in development, so maintenance and sustainability activities are still very vague

[60] Ref for 21 CFR 820 Quality system regulation

[61] Paper on current Computer System Validation practice – Good CSV Practice, pstestware, 2006

- Very vague estimates for support, training and change management facilities are available
- Agile development can be used as an excuse for missing accurate requirements engineering or management, especially alignment and risk assessment with GCP criteria not met
- Requirements establishment is missing a strong driver or community
- Quality Management/assurance not fully implemented, all rather informal - is there evidence of greater organisational / institutional commitment to this
- A broader understanding of GCP-compliance, regulations and standards is missing
- Security requirements are partly met, no evidence that a risk analysis or impact analysis for patient's safety has been performed

For a detailed view on the observations made, please check the Appendix for evaluations plans per tool/service. The deviations listed above are not intended to be an all-inclusive list of deficiencies or weaknesses that may exist. It shall function as list to help and support the project to transform from a project to a fully professional supported product.

4.5 Software development as project or as product

Software as a Tool vs. Software as a Research Object - Possibilities of Realizing Oppositional Requirement Profiles within a Single System

4.5.1 General Project Approach

As with p-medicine, basically all research-oriented projects are founded on the well-known "scientific method", i.e. they are trying to extend the current state of knowledge by proposing novel hypotheses and developing methodologies and tools to test the validity of those hypotheses.

The main outcome of such projects is a plethora of diverse "information" documenting the chosen goals and approaches along with the attained results. Other researchers can then re-use, verify and augment those results in their own work. Often, the "information" is not disseminated only through scientific reports and publications but also forms the basis of software artefacts designed as test vehicles for the initial hypotheses. Therefore their principal purpose is on "show-casing" newly devised research methodologies or technologies and, consequently, they are mostly on the level of proof-of-concepts or prototypes which are indeed capable to demonstrate the viability of concepts and ideas yet inherently incomplete and unstable.

Obviously, these points are in stark contrast to the expectations of regular users towards the applicability of a piece of software in a "real-world" environment: They legitimately expect software tools to properly fulfil their everyday needs and requirements and feature a high degree of stability, safety and security. The latter receives even more profound significance in the case that software is to be used within a medical work setting where the processing of sensitive patient data is involved.

4.5.2 Exception to the Rule

With ObTiMA, the p-medicine project offers one particularity that might represent an exception to the above "rule": The goal for this piece of software is to offer both research-oriented features based on innovative yet potentially immature technologies but also industry-oriented features based on well-established and mature technologies at the same time. In that sense, ObTiMA is intended to be both as a software tool as well as a software research object.

Before going further, it must be noted that the development of ObTiMA had already started in p-medicine's predecessor ACGT[62]. At that time, its main objective was to highlight the potential of ontology-based data management and semantic mediation between independent software components. But the potential of ObTiMA to become a "proper" application system was realized quite early and thus the goal was set to elaborate it further into that direction. Still, the system should stay "cutting-edge" by including novel technologies developed within p-medicine.

As a consequence, it became necessary to plan how such apparently oppositional requirement profiles can be possibly realized within a single system. The following paragraphs try to explicate some of the issues encountered regarding this plan and describe some of the strategies and methods employed to mitigate those issues. Obviously, not all points are fully applicable to all other tools created within p-medicine yet some general rules can be readily deduced from the depicted approach and included in other tool developments as well.

Today, product development and regulatory compliance functions are usually conducted by different organizations in silos, using multiple information systems and manual processes. These critical functions often consume excessive amounts of time, and deliver less than optimal results because of the difficulty in exchanging information and a mutual lack of coordination. Product lifecycle management (PLM) has become a leading technology that allows companies to rapidly plan, organize, manage, and produce new products or services in an integrated way. For example, ENOVIA® PLM solution for life sciences offers an end-to-end solution, spanning the entire product development process as well as most of the quality systems processes[6364].

Integrating compliance and innovation is a critical business challenge. A number of manufacturers have implemented business systems designed to improve the performance of their critical product development and quality systems processes. However, almost all still implement these business systems incrementally as point solutions, to address a specific need. For example: one department fielding complaints might enter a complaint into a call management system; a second might enter the same complaints into a different system that formats them for reporting to the FDA; a third might use yet another method in order to analyse developments in data, with a further system to track and resolve corrective and preventative actions (CAPAs)[65]. A simpler and more integrated way of dealing with compliance has to be found; data should be entered or collected only once.

4.6 Usability by ECRIN as aim of the survey

According to the description of work of p-medicine, all tools that are being developed for p-medicine and which are intended to be used in GCP-compliant trials are subject to undergo a validation and certification process. In the p-medicine project already a number of evaluation and validation steps are performed. 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 Dr.Eye 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

[62] http://www.ehealthnews.eu/acgt

[63] Yang X, Moore P R, Wong c-B, Pu J-S, et.al.: Product lifecycle information acquisition and management for consumer products. Industrial Management & Data Systems, 107 (7), 936 - 953 (2007)

[64] Ming X G, Yan J Q, Wang X H, Li S N, et.al.: Collaborative process planning and manufacturing in product lifecycle management. Computers in Industry, 59, 154–166 (2008)

[65] Bridging the gap between compliance and innovation. 2012 Dassault Systèmes

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 is developed, evaluated and validated mainly within task 8.4. In addition, task 8.3 takes care of data deidentification and pseudonymisation tools and is therefore relevant for the integration of these services into data management. Task 5.1 supports software development in that it delivers the data protection and data security framework. Our usability assessment fits into this quality control efforts of the p-medicine project in that it assesses a potential use of p-medicine by ECRIN. For this purpose and as described in the text, a focus of our assessment was these requirements that a user/customer employs as part of a developer/vendor audit to evaluate the degree of quality management during tool development. To use an faultless software that will not harm the patient during operation and will not corrupt or eliminate valuable study data is a GCP demand and an aim of ECRIN.
Dr.Eye as an integrated platform will serve as a tool to perform in-silico clinical trials on cancer by allowing users to analyse DICOM images together with the visualization of multi-modality tomographic data. The DoW requires that the GCP criticality related to the software system is continuously detailed. Three levels for GCP criticality are considered “direct impact, indirect impact, and no impact” systems. Direct impact means that operation, query, data, control, alarm, or failure will have a direct impact on data quality of GCP data and may harm the patient. Indirect impact of the system means that the operation, query, data, control, alarm, or failure has not a direct impact on data quality of GCP data. Indirect impact means that they may have an effect on the performance or operation of a direct impact system. No impact is a system where the operation, query, data, control, alarm, or failure will not have neither a direct nor an indirect impact on data quality of GCP data.

4.6.1 Personalised medicine clinical trials at ECRIN centres

Discussions by experts from ECRIN and the EU project p-medicine and other experts in personalised medicine and IT management were conducted. These experts consisted to a great part of members of the ECRIN Data Management Working Group. It was discussed that services for personalised medicine are especially difficult to integrate into the highly complex and regulated clinical trial domain. For research in personalised medicine, it was recommended that comprehensive, accessible and interoperable datasets must be generated and therefore data management solutions have to collect and link data from very different sources like hospital data, biobank data, genetic data, imaging data, and clinical research data.
Following tools are developed by p-medicine to support personalised medicine and that may be used in ECRIN clinical trials: DoctorEye (image amendment), ObTIMA (clinical data management), tools to manage SAE/SUSAR (ObTiMA module), DSS (decision support system), tools to access biobanks (ObTiMA module), data warehouse, patient empowerment tool, and tools to manage DICOM image transfer (ObTiMA module). For integration into ECRIN clinical trial processes ObTiMA offers the highest value because it offers clinical data capture with biobank access management (ObTiMA) and connection to imaging. ObTiMA can not only be used for personalised medicine trials, but for all kinds of trials. An inovative feature of ObTiMA is an ontology based design of CRFs making it easier to create CRF for different disease domains. In addition, imaging gains more and more importance in clinical trials and an integrated image management service may enable new kind of trials that were previously not possible. An important requirement for ECRIN is that only validated tools/services can be used for clinical trials. System validation is a highly complicated process that is used for conventional data management systems and requires the creation of user requirements, a validation master plan, qualifications for installation, operation, performance, and developer evaluations. Because most ECRIN centres possess own CDMS, any new tool has to show an added value for ECRIN, to make clinical trial conduct easier, faster, more efficient or more secure. In case p-medicine acts as SaaS provider, the

requirement for GCP compliance extends to service provision. It must be ensured that SaaS providers follow GCP and the services are able to support GCP trials and can seamlessly integrate into GCP compliant ECRIN clinical trial processes. For example, since ECRIN clinical trials are international, there is the need to ensure that local regulations are followed and it is essential to know where the trial data is hosted. Therefore, the service provider should employ a service strategy, including service design (requirements for service levels, availability, security, continuity, and change), service operation (incident, access, service desk) and quality management in general. In addition, service validation and usability testing have to be performed for the services.

4.6.2 Agility and quality assurance

All p-medicine developers are using agile methodes. But the survey identified that what is often missing is a continous and documented quality management. It is an irrevocable requirement for ECRIN that all p-medicine tools and services are developed according to quality assurance principles. During the development of products and services, quality assurance is the systematic process of checking that a product or a service meets specified requirements. Especially critical projects may benefit from a strict quality management. Often companies have a separate quality department devoted to quality assurance. A quality assurance system is used to identify defects before they get into the final product. ISO 9000 is an international standard that many companies use to ensure that their quality assurance system is in place and effective. Conformance to ISO 9000 is said to guarantee that a company delivers quality products and services. To follow ISO 9000, a company's management team decides quality assurance policies and objectives. Of great interest for critical software development projects is the question whether agile methodologies can be successfully implemented in an academic environment and still provide the benefits. Often, agile software development has typically been applied to non-critical projects using relatively small project teams where there are vague requirements, a high degree of change, and no significant performance and usability requirements[66]

The agile method focuses on fast and individual projects; on the other hand, there are the more disciplined methods, focused on setting up organizational processes for getting projects done with predictable high quality. Using agile methods in their pure form for projects that need either high availability, high usability is considered too risky by many practitioners[67]. It was shown that individual agile techniques do not necessarily have to be associated additional risk for projects having higher availability, performance, and quality requirements. Agile methodes are seen to handle unstable and volatile requirements throughout the development lifecycle and to be able to result in software with fewer defects and errors, in shorter timeframes, and under predefined budget constraints.

Therefore the agile method seems to be well suited for the academic environment and thus for p-medicine. The iterative and incremental way of development allows both requirements revision mechanisms and customer/user active participation in the decision-making process. Customer participation provides the needed feedback mechanism, ensuring a better final product. However, lack of documentation and handling of existing quality defects and errors is a typical problem in agile software maintenance. The practice of test-driven development (TDD) can have a positive impact on the culture of quality assurance during development. In response to the increasing criticality of software within systems and the increasing demands required for software in the personalised medicine domain, increased emphasis has to be

[66] Boehm B, Turner R: Balancing Agility and Discipline: A Guide for the Perplexed. Addison-Wesley Longman, Amsterdam (2004)

[67] Kile J, Inampudi MR: Agile Software Development Quality Assurance: Agile Project Management, Quality Metrics, and Methodologies. In: Stamelos IJ and Sfetsos P (eds.): Agile Software Development Quality Assurance, Idea Group Pub (2007)

given to systems and software dependability; increasing connectivity and interoperability and increasing needs for software integration, all resulting in more complex sources for errors.[68] This problem points to the possible role of a QA tester in a Scrum team. Often the QA team handles system and acceptance testing, including both manual and automated tests of the software against requirements. Software design should already have an focus on the testability and correlating design with requirements, documentation, code and tests. The QA tester should report on the quality metrix for each iteration, identifying modules that are high in complexity, have low test coverage and a high error rate to indicate components where a thorough unit or integration test is needed. QA should not be an active part of the developer team. The core concept of any agile methodology is the continuous communication (Tab. 4). A misunderstanding for new QA managers moving from waterfall model to agile devlopement, is the idea that there aren't any specifications or guides to tell them how to test specific functionalities. Software developers often tend to ignore the fact that requirements are not fully representing the correct customer expectations or needs. Another difference in the traditional and agile approaches is the attitude to documentation. A lack of documentation could be detected in our survey. The Agile Manifesto[69] sees an higher value in a working software solution than in a comprehensive documentation. Thus ECRIN will not find detailed and elaborate requirements specifications, testing plans or quality plans in an agile development project. But the Agile methods do have ways to document their quality activities, often this is a short, electronic documentation. Several software application exits that can support agile development. For example, JIRA[70] is an issue tracking application, developed by Atlassian that can be used for bug tracking, and project management; Flyspray[71] is a web-based bug tracking system for with many functions to assist with software development. Indeed, agile development is much concerned about product quality in the sense of a “Fitness for use” rather than conformance to requirements.

Agile principles	**Possble significance for ECRIN**
Individuals and interactions are valued over processes and tools	ECRIN should cooperate with developers already in an early stage ECRIN should develop requirements at an early point of development
Working software is valued over comprehensive documentation	ECRIN’s developer assessment should adjust to the short, electronic documentation and variable requirements characteristic of agile development
Customer collaboration is valued over contract negotiation	ECRIN should cooperate and deliver input
Responding to change is valued following a plan	ECRIN should expect not to build on a comprehensive quality plan, SOPs, testing plan when performing a developer assessment

Tab. 4: Support of agile principles by ECRIN

[68] Boehm B: Some Future Software Engineering Opportunities and Challenges. The Future of Software Engineering 2010: Nanz S (ed.), Springer-Verlag Berlin Heidelberg, 1-32

[69] Manifesto for Agile Software Development (2001). Available online: http://agilemanifesto.org/principles.html

[70] https://www.atlassian.com/de/software/jira

[71] http://flyspray.org/doku.php

5 Discussion

5.1 Consequences for the use of p-medicine tools in ECRIN trials

The use of all p-medicine tools has to be validated for the p-medicine framework and for the use in ECRIN. Because the business model for p-medicine sustainability has not yet been decided, ECRIN doesn't know if the tools will be installed at an ECRIN centre or used as a service. Therefore, the usability assessment has to assume both models and eventually a mixed model. Nonetheless, for all kind of usages the most important requirement of ECRIN is the GCP compliance of p-medicne tools. The usability of p-medicine tools will also be evaluated for the employment in an international clinical research infrastructure. Good clinical practice (GCP) is an international ethical and scientific quality standard for designing, recording and reporting trials that involve the participation of human subjects[72]. It ensures that the usage of software tools doesn't lead to a increased risk for the patient, protects patients rights and confidentiality, ensures the ethical conduct of biomedical research and that the data collected is of high quality. GCP compliance is a main usability criteria for the assignement of tools for usage in clinical trials.

Usability is the measure of the potential of software to accomplish the goals of the user covering the ease of use, visual consistency, etc.[73] In this way, usability should be part of the design process of software, keeping the needs of the user a central concern. Consideration of usability issues in the p-medicine project is part of the project's quality management and the developed tools are critically evaluated for their usability in the p-medicine environment. But because p-medicine tools will be integrated in the clinical trials infrastructure ECRIN[74][75], to be used in international clinical trials, the usability concept has to be extended so that p-medicine tools can be evaluated for application as part of ECRIN clinical trials data management[76]. Users of the tools will be investigators at their clinical site of ECRIN clinical trials centres, and to some degree their representatives (e.g. study nurse), ECRIN data managers and monitors. In any case, compliance with GCP and applicable regulations will become part for the usability as well as international aspects for the investigators[77]. Thus the usability concept relevant during software design, covering topics like ease of use, likeability and usefulness, has been extended in p-medicine so that it covers conditions of hospital data, confidentiality, use of source documents, as well as standard operating procedures and quality control during data handling to ensure that all data are reliable.

5.1.1.1 The ECRIN Standard and ECRIN certified data centres

ECRIN (European Clinical Research Infrastructures Network) is a European network providing support through different national partners (e.g. DCRIN, KKSN, INSERM, EIT, SweCRIN) for international clinical trials. ECRIN is creating certified ECRIN data centres that are able to provide GCP compliant data management. For this certification process the

[72] Good-clinical-practice compliance: http://www.emea.europa.eu/ema/index.jsp?curl=pages/regulation/general/general_content_000072.jsp&mid=WC0b01ac05800268ad

[73] Definition by TechTarget, http://searchsoa.techtarget.com/definition/usability

[74] Demotes-Mainard J and Kubiak C: A European perspective--the European clinical research infrastructures network. Ann Oncol. 2011 Nov;22 Suppl 7:vii44-vii49

[75] Demotes-Mainard J and Ohmann C: European Clinical Research Infrastructures Network: promoting harmonisation and quality in European clinical research. Lancet. 2005 Jan 8-14;365(9454):107-108

[76] p-medicine Del6.2: Evaluation report of the usability of p-medicine tools within the ECRIN infrastructure (30.1.2014)

[77] Kuchinke W and Ohmann C: A technical introduction to the basic requirements of clinical trials. EJHPP, Volume 15, 2009/5:20-22

"Working Group on Data Centres" of ECRIN has developed a standard describing the requirements of GCP-compliant data management in multinational clinical trials[78]. These requirements are divided into two main parts: an IT part covering standards for the underlying IT infrastructure and computer systems in general, and a Data Management (DM) part covering requirements for data management applications in clinical trials. In 2012 the ECRIN standard has been used for two pilot audits of ECRIN data centres and more audits will follow. The development of the ECRIN standard was initiated by a perceived lack of clarity to ensure GCP compliance for clinical trials data management and the existing heterogeneity of academic clinical trial data centres[79]. The aim was to bring ECRIN and other data centres to the same level of quality and standardisation and to make them evolve towards a common standard quality level. Meanwhile a substantial revision of the original ECRIN standard has been completed in 2012[80] and two centres have been successfully certified (Uppsala and Düsseldorf). The standard provides a clear interpretation of regulatory and good practice requirements, in the context of the limited resources available to non-commercial trials units in Europe, and so act as a general guide to establishing and managing high-quality data management services. Because ECRIN is a partner in several projects, the standard will also be used for the interoperable integration of ECRIN data management with new tools and services.

System validation plays an important part in ensuring GCP-compliance of a computer system, but can be problematic. Academic units do not, in general, have the resources available in the pharma industry to conduct or outsource a 'full' validation for every system component, including the vendor assessment (audit), and to maintain complete change management. In addition, there is no simple way to know how much system validation is necessary or sufficient[81] and the extent and depth of validation required may depend on the interpretation of a particular auditor and whether a commercial software, an own developed software, a service or a SaaS is used. Here the certified ECRIN data centres can play an important role. These centres were certified for GCP compliance and the ability to conduct international trials. Thus, the ECRIN data centres are well prepared for an GCP audit and to become a partner for p-medicine to support p-medicine in their compliance tasks. The ECRIN standard requirements list was the basis for the certification of ECRIN data centres. Certification as an ECRIN approved data centre demonstrates, first, compliance of the certified centre with regulations and standards, including GCP; second compliance with recommendations of ECRIN in terms of data management; third, that the centre is staffed by expert personnel, and fourth, that the centre is competent in the management of data for international, multicentre clinical trials. Thus, by implementing the certification procedure based on requirements that are GCP-compliant, ECRIN can guaranty a standard quality level for data management performed by academic trial units in pan European trials. A part of the standard was consulted for the developed questionnaires. The standard is of limited use for the assessment of single tools, but has to be used for data centres. In this way, the standard may be valuable for the assessment of STaRC. In may be possible that STaRC can apply to be certified as a data centre. To receive such a certificate, it is a useful preparation to assess the GCP compliance of p-medicine tools that is done as part of this deliverable.

[78] Ohmann C., Kuchinke W., Canham S., et.al.: Standard requirements for GCP-compliant data management in multinational clinical trials. Trials 2011, 12:85 (22 March 2011), available online: http://www.trialsjournal.com/content/12/1/85

[79] Kuchinke W, Ohmann C, Yang Q, Salas N, Lauritsen J, et.al. Heterogeneity prevails: the state of clinical trial data management in Europe - results of a survey of ECRIN centres. Trials. 2010 Jul 21;11(1):79-89

[80] Ohmann C, Canham S, Cornu C, Dreß J, Gueyffier F, Kuchinke W et.a.: Revising the ECRIN standard requirements for information technology and data management in clinical trials. Trials 14: 97 (2013), online available: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3653810/

[81] Mullendore B: Computer Validation Master Planning - Technical Guide, IVT Press 2002

Usability is evaluated by the quality of communication (interaction) between a technological product (system) and a user (the one who uses that technological product)[82]. The unit of measurement is the user's behaviour (satisfaction, comfort, time spent in performing an action, etc.) in a specific context of use (natural and virtual environment as well as the physical environment where communication between user and technological product takes place). The usability concept and its measurement are strictly connected to that of accessibility, and the space of the problem, shared by the users, in which the interaction takes places. For this reason we modelled the requirements necessary for a clinical trial using imaging and biobanking processes. Because ECRIN has not yet conducted a personalized medicine trial, the corresponding requirements are missing in the ECRIN standard. Nonetheless, it was possible to list the possible requirements for a personalized medicine trial with the inclusion of biosamples management and image endpoints to be used for the assessment of p-medicine biobank tool and image tool (Dr.Eye).

The evaluation described in this report shows that the p-medicine tools are not yet ready for operation and employment in ECRIN. No single tool has reached the candidate status. Furthermore, a GCP compliant use of p-medicine tools requires the provision not only of the tool, but also additional services for maintenance, training and further development. The business model analysis showed no definite result; it is unclear how p-medicine tools will be made accessible to users. The most probable solution will be a mixture of Open Source provision of core components and service provision. This has for the use of p-medicine tools in ECRIN consequences.

The results show the necessary of the integration of data services to the data management in clinical trials to enhance data management that is GCP (Good Clinical Practice) compliant at ECRIN Data Centres. The provision of services, often cloud based services, is a new development in the Life Sciences. One of the major concern of cloud based service provision is compliance. It must be ensured that cloud service providers that are used by service consumers follow GCP and relevant regulations, to ensure the system is fit for its intended use. This implies that a cloud based service system must include IP/IQ (installation protocol and installation qualification), OQ (operation qualification) and PQ (performance qualification) that are combined the required products of any computer system validation. System validation of a clinical cloud application means that the service consumer cannot have an installation protocol for installation of the hardware. In addition, the service provider must deliver test and production environments for each application in the cloud. Backup and restore functions must be implemented and tested for all production applications. Even the computer system validation of the tool must take place in the cloud. The same documentation and methods has to be used as if the application was running on a local server. Since clinical trials are more and more international, there is also a need to ensure that local regulations are followed. For example, it is essential to know where the data is hosted. Indeed some countries require the clinical data to be hosted in the actual country of the clinical trial. The service provider has to employ a service strategy, including processes and policies for service design (service level, availability, security, requirements, continuity, change), service operation (incident, access, service desk) and quality management. In

[82] Federici S and Borsci S: Usability evaluation: models, methods and applications. In: JH Stone, M Blouin, (eds). International Encyclopedia of Rehabilitation. Available online: http://cirrie.buffalo.edu/encyclopedia/en/article/277/

addition service validation and usability testing have to be done[83]. Compliant service provision will be challenging for many academic service providers. In clinical trials, the service consumer is the investigators at the clinical trial center, but also the trial sponsor (leading investigator) and the monitor.
For clinical trials in personalised medicine, additional participants like laboratories, biobanks and centres of excellence (e..g. for image analysis or DNA sequencing) have to be considered. In general, compliance with “Good Clinical Practice” (GCP) is a prerequisite for the execution of many clinical trials (e.g. for medicinal products) and increasingly it is recommended for all types of trials. One requirement for GCP trials is that the employed Clinical Data Management Systems (CDMS) must be compliant with GCP and this compliance must be demonstrated by a process called “system validation”. GCP competence in personalised medicine means that all tools and data flows that are concerned with the patient data must be included. This may become quite complicated, because for example, a prerequisite for the efficient employment of personalised medicine is the joint use of a large number of tools for data mining, data analysis, biobanking, data collection, disease modelling, scenario simulation, storing of genomic information, and data sharing with care data (e.g. EHR data).
The interoperable integration of new tools or/and services developed by p-medicine will enable ECRIN to support the conduct of personalised medicine trials and in this way will expand the capabilities of ECRIN data management. Because these personalised medicine tools will be mostly provided as services, ECRIN must find a sustainable way to integrate them into the established ECRIN clinical trials processes and into the ECRIN GCP compliant data management infrastructure.
In a service based infrastructure the service provider receives more responsibilities for installing, running and maintaining a system for GCP compliance. The report recommends that p-medicine as a service provider will provit when GCP compliance is built into their tools/infrastructure and the service provision framework. Our analysis points to the problem for sustainability of a personalised medicine research infrastructure. Once tools or application are provided, integration with local systems as well as support/maintenance/help desk have to be provided and users must be trained. For the service provider, these investments must pay off by an extended and efficient use of the services in clinical trials. The system validation has to done by the service provider. We propose that clinical trials services should be designed for sustainability. This may be acchived by aligning of service provision with a business model. This would help to justify strategic investments, the use of resources for implementation and training, and guarantee sustainability. Part of this business level integration would be the SLA management.
An important result of the assessment is the identification of weeknesses in the documentation of quality management and the development processes. All p-medicine developers are using agile methodes where the documentation is always a problem. What is often missing is a documented quality management and corresponding tests. But the future user/purchaser of the software needs for the developer assessment prove of the quality of the product: all p-medicine tools and services must be developed according to quality assurance principles. Thus, of great interest for the software developer is the question whether agile methodologies can be successfully implemented in an academic environment and deliver the necessary quality assurance documentation. We are convinced that agile methods are well suited for the academic environment (software as a project) and may also be used for the quality management (agile quality management) when the agile methology is adapted to the volatile environment of agile development. Agile quality management may

[83]Wolfgang Kuchinke: Integration of Data Services to Enhance Clinical Trial Data Management and GCP (Good Clinical Practice) Compliance at ECRIN Data Centres. Proceedings of eChallenges, echallenges.org/e2013 (2013)

imply for example involvement of the product owner for QA, daily meetings between developers and QA, little but constant documentation. QA processes and documentation should also be iterative and incremental with tight collaboration between developers and QA people and active participation customer/user. In this way test-driven development (TDD) may be developed with an positive impact on the depth of quality assurance during development. Nonetheless, risk assessment has to play an important role in every step of the agile development process. Using feed back of user requirements and specifications to the developer group will enable developers to incoporate compliance into the software to ease the transition from software as a product to software as a tool/service (Fig. 9). Based on the assessment of the survey, recommendations were developed that suport this process and give tips for effective quality management in an agile development environment (chapter 6.1).

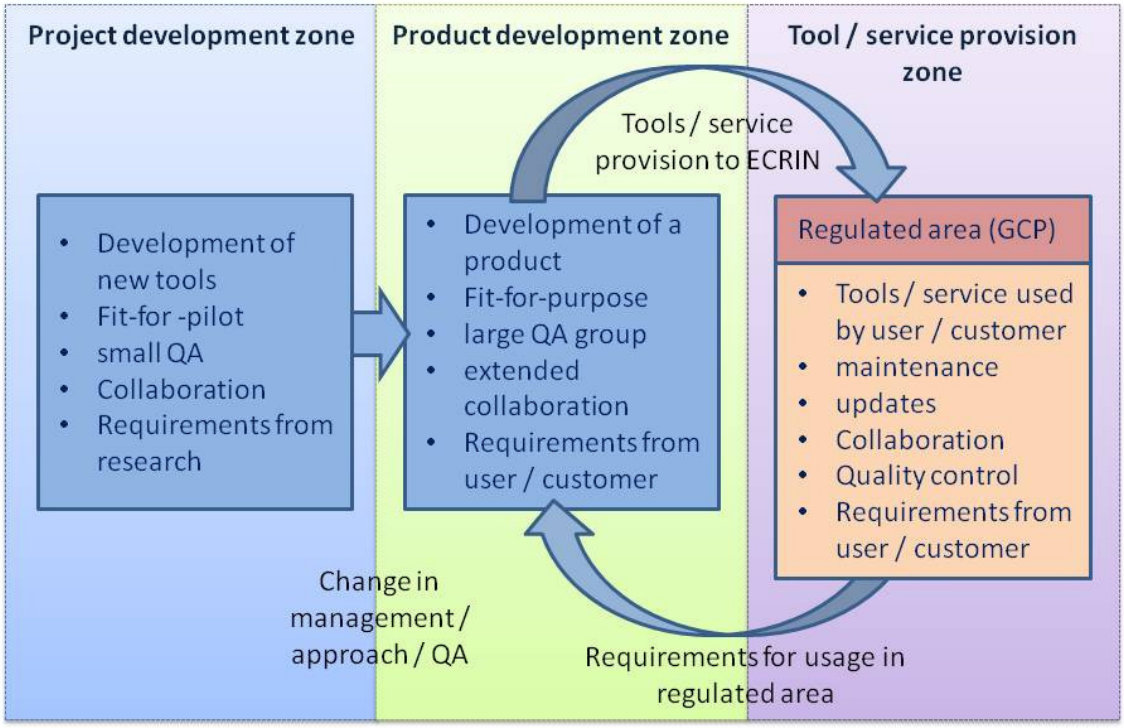


Fig. 9: Model of the feedback of user requirements to the developer group to enable a smooth transition from software as a project to software as a product to the tool/service provision

One aspect that must be discussed in this context is how to finance improvements in QA in an academic developer group where resources are always limited. Because an increase in the number of developers or QA persons seems not possible, persons could collaborate more intensely (for example: cross developer group reviews or audits), use of software like (Document Control Software, Quality Management Software, Audit Management Software, User Complaint Software), employ forms of agile QA (daily meetings with QA, little but constant electronic documentation), use where possible automatic documentation of processes, tests, etc. (see: recommendations, chapter 6.1).

6 Consequences

6.1 Recommendations for the p-medicine project

The consequence of our evaluation of p-medicine tools for the use in ECRIN clinical trials is that at the present date the tools cannot be used in ECRIN. Due to the fact that p-medicine tools are still in development, a use in ECRIN trials cannot be recommended at the moment. In addition, the integration and employment of the tools in ECRIN will become a challenge. Therefore, based on the evaluation, recommendations were developed that may simplify the employment of p-medicine tools in ECRIN in an regulated environment. The following recommendations should give p-medicine guidance and assistance for the rest of project lifetime to evolve from an "academic" driven consortium to a professional service or tool provider for clinical trials.

6.1.1 Recommendation "Quality Management/Assurance (QA)"

As the reliance on computer systems to deliver operational solutions continues to grow, the primary business benefit of QA is to promote risks system quality. QA ensures the quality and reliability of a computer system. This process focuses on the detection and prevention of defects starting already from the **beginning** of a project (SDLC approach). A well-documented and continuously developed QA, will reduce system functional and operational problems, business process problems, and finally the **harm to patients**. p-medicine should consider to employ dedicated quality managers, that deal with quality management aspects for the on-going development projects. The p-medicine quality manager should establish controlled documents such as SOPs for development, testing, change and configuration management and consider also responsibilities and roles within the project. It should be considered that documentation in an agile environment needs not to be extensive but can be concise. The cross project establishment of a quality manager should as a first step implement an overall software development plan, which compromises following aspects:

- Roles and responsibilities
- Software Development Modell, such as SCRUM
- Software Change and Configuration Management
- Testing policies and procedures
- System / software documentation
- Requirements engineering and management
- Integrated risk assessment
- Considering GCP and security requirements from the beginning on
- Assessment approach of GCP relevant functionality or components

6.1.2 Recommendation "Risk assessment accompanies the development life cycle"

Different types of risk assessment should be used to accompany the development of the software (SDLC). Basic risk assessment should beginn already during software design phase, followed by functional risk assessment and GCP focused risk assessment during IQ, OQ and PQ, and after the tool has been developed, the checking of risks during the operation phase.

6.1.3 Recommendation "GCP training for developers"

We recommend that all developers working in p-medicine shall be trained at least internally to fully understand GCP and the aims/objectives of computer systems validation (CSV). The evaluation revealed a missing sensibility of developers for GCP relevancy. This is not

surprising, because CSV is based on the interpretation of rather generic GCP principles and normally done by experts. To avoid this ignorance in future, a formal GCP training should be considered that is adapted to the needs of developers. p-medicine tools / services will replace our current mode of medicine over the coming years with a personalized **predictive** treatment based on tools, services or basically on algorithms that deal with patient data. Any developer shall be clearly advised, instructed and trained that any functionality or component that processes, transfers or transforms patient data and has an impact on the treatment of the patient may cause harm to the patient and shall be assessed and analysed accordingly to GCP.

6.1.4 Recommendation "Knowledge Transfer regarding Computer System Validation"

The information regarding the computer system as well as what will become necessary for system validation is already available within the p-medicine consortium, mostly in form of expertise and experience of the developers. We recommend to structure this knowledge and to thoroughly document the phases of the SDLC to be able to transfer the existing knowledge to those who will need it in using, supporting, maintaining or enhancing the system. The existing knowledge will be necessary to ensure and to support validation and maintenance efforts of the system after going live (live candidate). Through the use of a quality system that ensures the controlled documentation of knowledge in forms of manuals, trainings, changes and configurations, the knowledge will remain in the organisation even if key developers leave the organisation.

6.1.5 Recommendation "Business Plan"

ECRIN is a network of academic clinical research organisations, which are conducting clinical trials as part of their business. For the usability in ECRIN, ECRIN should have an added value by using p-medicine tools in their infrastructure. The future business organisation (e.g. Starc) that will promote p-medicine tools / services should reflect these demands in their business model. At least following aspects should be reflected in the business model, business plan and corresponding business processes:

- Business strategy and vision
- Service portfolio and products
- What services or tools will be provided?
- How can these tools integrated into the clinical research infrastructure?
- Added value of provided tools/services
- Added value of business organisation carrying out p-medicine tools/services
- Pricing models for provided services/tools
- Licences
- Service models, such as "software"-, "platform" and "infrastructure" as a service
- How will these services billed? (e.g. pay per use, pay per volume, pay per transaction)
- Dynamic vs. static pricing models
- Support, help desk and training
- Will training courses be offered?
- Will there be 24/7 help desk?
- Telephone or email support?
- Technical support?
- Validation support for integration into clinical research infrastructure
- Will manuals provided to support validation efforts?
- Will validation support offered?
- Commitment to QA/QM
- Certification or Accreditation of tools and services?

- How will be proved how the tools have been developed in accordance with regulations?
- Security
- Business Continuity
- How will the tools be sustainable for 3, 5 an 10 years?

6.1.6 Recommendation “Requirements Engineering”

There is no evidence that the envisaged users’ demands (future purchasers, users) will be adressed accordingly; this should be carefully analysed and a strategy for more enduser integration should be established. To avoid development that does not accuratly adresses these needs, we recommend to establish an user community to be able to prioritise requirements. Further the evaluation revealed that the requirements engineering process is not driven carefully with close interaction of management and with a robust business perspective. For an agile development approach, it is essential that the product owner is integrated very closely, on a daily basis. Otherwise it should be considered to use another software development model, if this is not possible.

6.1.7 Recommendation “Agile Development”

Agile development, such as SCRUM, is a very clearly defined model with clear roles, responsibilities and activities through the whole project lifetime. If the end user is not able to closely collaborate on a daily basis, we recommend to use a different development model, with less collaboration between end users and development staff during development. Otherwise the project will not profit from the advantages of agile development. We recommand to consider to use an approach that decouples the requirements engineering phase from the development phase.

6.1.8 Recommendation “Integrated Risk Assessment”

An integration of risk assessment procedures at every step of the SDLC can make it manaeable to deal with the increased demands for documented QA. Only critical components have to be tested in full depth. Risk assessment should already begin with the software design pahse.

6.1.9 Recommendation “Build-in-Compliance”

Tight collboration with ECRIN as enduser of p-medicine tools may provide all requirements and specification necessary for the developers to consider GCP and regulatory compliance already during the development process and in this way to build compliance into the system. One aspect of this approach that it supports the automatic generation of quality reports where this is possible.

7 Appendix

7.1 Risk Assessment tables

7.1.1 Risk analysis template

Risk Analysis							
Risk Analysis	Description/ cause	Probability (high/mediu m/low)	Impact on single tool (high/mediu	Impact on p-medicine (high/mediu	mitigation measures (preventive	contingency measures (what to do if	responsible team/person

7.1.2 Risk analysis ObTiMA

Risk Analysis: OBTIMA							
Risk Analysis	Description/cause	Probability	Impact on single tool	Impact on p-medicine	mitigation measures (preventive measures)	contingency measures (what to do if risky situation occurred)	responsible team/person
Server misconfiguration	The configuration of the server running ObTiMA is faulty. This can lead to unexpected and faulty application	medium	high	low	Detailed records of server configurations must be available, with logs of subsequent updates.	Fix the misconfiguration based on the records available. Check data for loss or corruption - repair if necessary or import backup if repair not possible.	ObTiMA
Server crash (software)	The operating system fails unexpectedly and shuts down the server.	medium	high	low		Check the reason for the crash and fix if possible. Check data for loss or corruption - repair if necessary or import backup if repair not possible.	ObTiMa
Server crash (hardware)	There is a faulty hardware that unexpectedly shuts down the server.	low	high	low	Hardware support arrangements should be in place to allow equipment to be replaced or repaired quickly.	Fix or replace the faulty hardware. Check data for loss or corruption - repair if necessary or import backup if repair not possible.	ObTiMA
Server theft	The server is physically stolen.	low	high	low	Servers must be housed within a dedicated locked room with unescorted access limited to specific roles, known to and reviewable by the centre.	Call the police!	ObTiMA
Server hack	Unauthorized persons gain (software) access to the server.	low	high	low	Clinical data relating to individuals should only be stored on protected servers and storage devices. It should not be stored on non secured devices (e.g. on laptops, desktops, USB	Check data for loss or corruption - repair if necessary or import backup if repair not possible. Check how the unauthorized persons gained access and close found security holes.	ObTiMA
Server non-responsive	The server is not responding to user requests because e.g. the operating system is hung.	medium	medium	low	Failure of any server directly supporting clinical trial activity, within normal local business hours, should result in alerts being sent automatically to relevant personnel	Check and fix the cause for the un-responsiveness. Check data for loss or corruption - repair if necessary or import backup if repair not possible.	ObTiMA
Improper handling of access credentials	Persons that have access to the server share their credentials illicitly.	low	high	low	The centre and its staff can demonstrate compliance with and commitment to all relevant data protection legislation, including the provision of related training	Change credentials to the server for the affected persons. Check for inappropriate data access and fix irregular changes.	ObTiMA
Data not sent through encrypted connection	The connection from the client to the server is not encrypted and thus all data are sent unencrypted.	low	medium	low	Clinical data transmitted over the internet to or from the trials unit should be encrypted	Check whether unauthorized persons had access to the data.	ObTiMA
Unallowed access to the server	Persons that have no expressed rights to access the server do so.	low	high	low	Each system requiring access controls should have mechanisms, e.g. using roles, group membership, etc., that can be used to effectively	Check whether only authorized persons with the necessary rights to access particular data accessed them. If not then check the data for correctness.	ObTiMA

7.1.3 Risk analyse of p-medicine portal

Risk Analysis: Portal							
Risk Analysis	Description/cause	Probability	Impact on single tool	Impact on p-medicine	mitigation measures (preventive measures)	contingency measures (what to do if risky situation occurred)	responsible team/person
The host server crashes	The portal server crashes because of hardware problems	medium	high	high	(a) Regular back-up of the portal instance, configuration files and the portal database; (b) Having a ready for usage backup server	(a) Setup a new server and make sure that it properly works and fix the primary server in the meantime; (b) make sure the back-up server runs and that it properly works and fix the primary server in the meantime	IBMT
Accessing the portal is not possible	The portal instance is not accessible because after after a power breakdown not all services have been automatically started	medium	high	high	Regularly check skripts for starting the portal instance and related Data Mining services automatically	Start the portal instance and related Data Mining services manually; check skripts for automatically starting.	IBMT
Single Sign-On is not possible	After logging in in the portal a user have to login in a p-medicine tool (e.g. ObTiMA) again	medium	high	high	Configuring user credentials in the p-medicine tools correctly	Example ObTiMA: make sure that the user id is correctly entered in the ObTiMA database; check Single Sign-On	p-medicine tool developers, e.g. UdS
Login in the portal is not possible	Login in the portal is not possible because the Identity Provider server is not running	medium	high	high	Having a messaging system for getting information if the server is not running	Restart the Identity Provider server and make sure that it properly works	CUSTODIX
Creating an account in the portal is not possible	A new user enters a wrong e-mail address on a registration form and never receives a confirmation e-mail for activating his account	low	low	low	(a) the user has to enter his e-mail address two times; (b) the user will see the entered e-mail address again for checking it; (c) the user will be informed about a time limit for waiting for the confirmation e-mail; (d) providing a global p-medicine support email address in the portal.	After expiration of the time limit for waiting for receiving a confirmation e-mail, the user can contact an admin or e.g. mail a global p-medicine support email address	IBMT; CUSTODIX

7.1.4 Risk analysis of OA

Risk Analysis: Ontology Annotator							
Risk Analysis	Description/cause	Probability	Impact on single tool	Impact on p-medicine	mitigation measures (preventive measures)	contingency measures (what to do if risky situation occurred)	responsible team/person
server crash	the server that hosts the ontology annotator crashes	high	high	low	software is deployed in secondary server	switch link in p-medicine portal to secondary server. Change would be transparent to users	UPM
hdot not accessible	the page storing the HDOT files becomes unaccesible	medium	high	high	the OA maintains a local copy of the HDOT files	the OA can work with the local copy of HDOT without any configuration modification	UPM
internal database server crash	the server hosting the OA database crashes	high	high	low	database can be deployed on a secondary machine	deploy copy of database, switch OA configuration to access new database server	UPM
internal database data loss	there is a permanent loss of data in the OA database that stores the OA projects	low	high	low	database is periodically backed-up	recover database with back-up data	UPM
inability to deploy in future machine configurations	due to third-party software updates, in becomes impossible to deploy the OA	low	medium	medium	keep dependency on third-party APIs as low as possible	search for replacement of outdated APIs	UPM
modification of interfaces with other tools in p-medicine	other tools in p-medicine modify their interfaces	low	high	medium	design OA architecture so change of interfaces affects as few parts of the code as possible. Define wrappers for those interfaces	update the wrappers to work with new interface configurations	UPM

7.2 Software Maturity Assessment

7.2.1 Software Maturity Assessment Matrix

	No.	Stage	Maturity	Reference documents	Involvement of ECRIN	Evaluation method (additive)
Testing/ Development	1	Pre-Alpha	Concepts, Architecture, Requirements Engineering, Software Design, Software Development initiated	Vision document, ideas, concepts	No	Evaluation of concepts, Requirements evaluation (Behaviour tree, Matrix, …)
	2	Alpha	Unstable, raw source code, subset of basic functionality, data loss, proof of concept	Core requirements specification, rudimentary software development process, software design, raw source code, test scripts + data (white box testing)	No	Functional testing, Interface evaluation (ISO 9241-110:2006)
	3	Beta	Basic functionality, unstable, performance/ speed issues, data loss, usability issues	QM, software development process, delivery process, change-request-management, feature set, bug tracking, usability tests, test plans (black box testing)	No	Quantitative evaluation (activity diagram ↔ software support)
	4	Release Candidate	Basic functionality, minor bugs, feature set completed/ closed, code completed	Closed feature set, user manual, installation procedure manual, operational procedure manual, process procedure manual, test scripts + data, assessment of usability	ECRIN experts	Validation Simulation, Qualitative evaluation (data flow ↔ software support), Test trial, SOPs, Gap analysis
Release	5	(Live-) Release	No known bugs, optimised (speed/ performance), high usability, adaption customisation needed Very stable, productive system, used by end-user	Support, “Enterprise edition”, SLA, Accounting, Pricing, GCP-Validation, developer evaluation, provider assessment, maintenance, support, user training	ECRIN experts	Validation Simulation, Test trial vs. requirements, IQ, OQ, PQ, user requirements validation, developer evaluation

7.2.2 Questionnaire: Tools maturity results

7.2.2.1 DEVELOPER INTERVIEWS

	ALGA-C	Data Upload Tool	ObTiMA	Ontology Annotator	p-BioSPRE	Trial Biomaterial Manager	Workbench
Software Development Process							
Maturity status	**β**	**α**	**RC**	**β**	**β**	**β**	**α**
Continuous Delivery							
Continuous Performance Management							
Continuous Development	X	X	X				X
Continuous Integration			X				
Continuous Deployment			X				
Specification							
Requirements Specification	X	X*	X*	X		X	X*
Reference Implementation documents			X				
Installation Manual		X	X	X*		X	
User Manual	X	X	X*	X	X	X*	
Validation master plan				X			
Risk analysis							
Testing							
Usability Testing	X	X	X				X
Integration Testing			X				

Load Testing			X*				
Testing Plans			X		X*	X*	
Testing Scripts			X				
Testing Data			X	X			

Quality Management and support documents							
Quality Assurance	X		X	X	X	X	
Quality Plan			X				
Quality Control	X	X	X	X	X	X	X
Training/ Education		X*	X*	X*	X		X*
Hotline							
Maintenance			X				

α = Alpha; β = Beta; RC = Release Candidate

* planned or in progress

7.2.2.2 ASSESSMENT

Software Development Process	6	*
Pre-Alpha	0	0
Alpha	1	0,5
Beta	3	1,5
Release Candidate	5	2,5
Live-Release	6	3

Continuous Delivery	6	*
Continuous Performance Management	1,5	0,75
Continuous Development	1,5	0,75
Continuous Integration	1,5	0,75
Continuous Deployment	1,5	0,75

Specification	6	*
Requirements Specification	1	0,5
Reference Implementation documents	1	0,5
Installation Manual	1	0,5
User Manual	1	0,5
Validation master plan	1	0,5
Risk analysis	1	0,5

Testing	6	*

Usability Testing	1	0,5
Integration Testing	1	0,5
Load Testing	1	0,5
Testing Plans	1	0,5
Testing Scripts	1	0,5
Testing Data	1	0,5

Quality Management and support documents	**6**	*****
Quality Assurance	1	0,5
Quality Plan	1	0,5
Quality Control	1	0,5
Training/ Education	1	0,5
Hotline	1	0,5
Maintenance	1	0,5

7.2.2.3 EVALUATION

	ALGA-C	Data Upload Tool	ObTiMA	Ontology Annotator	p-BioSPRE	Trial Biomaterial Manager	Workbench
Software Development Process	**3**	**1**	**5**	**3**	**3**	**3**	**1**
Maturity status	3	1	5	3	3	3	1

Continuous Delivery	**1,5**	**1,5**	**4,5**	**0**	**0**	**0**	**1,5**
Continuous Performance Management	0	0	0	0	0	0	0
Continuous Development	1,5	1,5	1,5	0	0	0	1,5
Continuous Integration	0	0	1,5	0	0	0	0
Continuous Deployment	0	0	1,5	0	0	0	0

Specification	**2**	**2,5**	**3**	**3,5**	**1**	**2,5**	**0,5**
Requirements Specification	1	0,5	0,5	1	0	1	0,5
Reference Implementation documents	0	0	1	0	0	0	0
Installation Manual	0	1	1	0,5	0	1	0
User Manual	1	1	0,5	1	1	0,5	0
Validation master plan	0	0	0	1	0	0	0
Risk analysis	0	0	0	0	0	0	0

Testing	**1**	**1**	**5,5**	**1**	**0,5**	**0,5**	**1**
Usability Testing	1	1	1	0	0	0	1
Integration Testing	0	0	1	0	0	0	0
Load Testing	0	0	0,5	0	0	0	0

Testing Plans	0	0	1	0	0,5	0,5	0
Testing Scripts	0	0	1	0	0	0	0
Testing Data	0	0	1	1	0	0	0

Quality Management and support documents	**2**	**1,5**	**4,5**	**2,5**	**3**	**2**	**1,5**
Quality Assurance	1	0	1	1	1	1	0
Quality Plan	0	0	1	0	0	0	0
Quality Control	1	1	1	1	1	1	1
Training/ Education	0	0,5	0,5	0,5	1	0	0,5
Hotline	0	0	0	0	0	0	0
Maintenance	0	0	1	0	0	0	0

7.2.3 Software Evaluation Questionnaire/ Checklist Template

General Information	
Software Name	
Tool / module	
Developer / Contact	
Version for evaluation	

Description	

Software Development Process		
	The frozen and evaluated version will be:	
☐	Pre-Alpha	Concepts, architecture, requirements engineering, software design, software development
☐	Alpha	Unstable, raw source code, subset of basic functionality, data loss, proof of concept
☐	Beta	Basic functionality, unstable, performance/ speed issues, data loss, usability issues
☐	Release Candidate	Basic functionality, minor bugs, feature set completed/ closed, code completed
☐	Live-Release	Very stable, productive system, used by end-user, no known bugs, optimise (speed/ performance), high usability, adaption customisation needed

Organisation/ general aspects	
☐	Business plan
☐	Previous audits or inspections
☐	Source code available for evaluation

☐	Escrow agreement available
☐	Other: …….

Continuous Delivery	
☐	Continuous Performance Management
☐	Continuous Development
☐	Continuous Integration
☐	Continuous Deployment

Specification	
☐	Requirements Specification
☐	Reference Implementation documents
☐	Installation Manual
☐	User Manual
☐	Validation master plan
☐	Risk analysis

Software, tool or service provision

☐	Tool / module
☐	Application Service Provider (ASP)
☐	Software as a Service (SaaS)
☐	Full service
☐	Others: ……

Testing (following testing documentation for tools will be provided)	
☐	Usability Testing
☐	Integration Testing
☐	Load Testing
☐	Testing Plans
☐	Testing Scripts
☐	Testing Data

7.3 Evaluation sheet for development practices / Criteria matrix

Area	#	Criteria	Status	Evaluation	Observation	Criticality
Development Practice	1	SOPs or equivalents exist covering development procedures, roles, responsibilities etc.	mandatory	o		
	2	SOPs or equivalents exist covering software change and configuration management	mandatory	-		
	3	A development plan is being used for the system(s) currently in development, in line with stated policies and methodologies	mandatory			
	4	Functional specification documents available and used as part of the development process	mandatory			
	5	SOPs or equivalents covering testing, continuous integration (CI), sign off / deplyment procedures etc.	mandatory			
	6	Modern source control implemented (e.g. Git, Subversion, Mercurial)	mandatory			
	7	Unit testing used and integrated with development and CI	mandatory			
	8	Integration testing used and integrated with development and CI	optional			
	9	There is evidence of peer review / support amongst developers	optional			
	10	System has been stress tested under high data load	optional			
Validation	11	Functional specification documents are available to users to support validation in their own environment.	mandatory			
	12	Validation scripts are avalable to users to support validation in their own environment	optional			

Non-Functional Aspects	13	Managing and ensuring security is part of the functional specification and / or development plan (e.g. anti-SQL injection)	mandatory			
	14	Error handling / logging / reporting part of the functional specification and / or development plan (but not optional!)	mandatory			
	15	Access control aspects part of the functional specification and / or development plan (e.g. authentication and authorisation mechanisms)	mandatory			
	16	System should record the access control authorisations managed within it	mandatory			
	17	System allows selected data to be stored encrypted	optional			
Regulatory compliance	18	The system can support audit trails for data as defined by GCP	mandatory			
	19	The system can display, report data and audit data in forms that support inspection and audit	mandatory			
	20	The system can support recording of source data verification	optional			
	21	The system can support blinding of intervention type when necessary	optional			
	22	The system can support pseudonymisation of data	optional			
	23	The system can support electronic signatures if necessary	optional			
User Support	24	Training courses are available to users	mandatory			
	25	Training materials and system documentation is available to users	mandatory			
	26	A test / demo installation is accessible	optional			
	27	Help desk / response facilities can be arranged	mandatory			
	28	Technical documentation is available to users	mandatory			
	29	Technical support arrangements are available	mandatory			
	30	Installation specification and documentation is available to users	mandatory			
	31	On-site Installation support is available	optional			
Ongoing Development	32	System providers have a commitment to / capability for ongoing bug fixes	mandatory			
	33	System providers have a commitment to / capability for ongoing development	mandatory			
	34	Functional specification of updates will be made available	mandatory			
	35	Test scripts will be made available for updates	optional			
	36	System should include mechanisms for reporting bugs and making feature requests	optional			

7.4 Abbreviations and acronyms

ACGT	Advancing Clinico-Genomic Trials on Cancer
BBMRI	Biobanking and Biomolecular Resources Research Infrastructure
BC	Bar code
CAPA	Corrective Actions and Preventative Actions
CDMA	Clinical Data Management Application
CDMS	Clinical Data Management System
CRA	Clinical Research Associate
CRC	Clinical Research Centre
CRF	Case Report Form
CSV	Computer System Validation
CTMS	Clinical Trial Management System
CTU	Clinical Trials Unit
DEISA	Distributed European Infrastructure for Supercomputing Applications
DICOM	Digital Imaging and Communications in Medicine
DoW	Description of Work
DSS	Decision Support System
EATRIS	European Advanced Translational Research Infrastructure in Medicine
ECRIN	European Clinical Research Infrastructure Network
EDC	Electronic Data Capture
HER	Electronic Health Record
ELIXIR	European life-science infrastructure for biological information
EMA	European Medical Agency
ENCCA	European Network for Cancer in Children and Adolescents
EORTC	European Organisation for Research and Treatment of Cancer
eSDI	electronic Source Data Interchange
ESFRI	European Strategy Forum on Research Infrastructures

FDA	Federal Drug Agency
FP7	Seventh Framework Programme
GAMP	Good Automated Manufacturing Practice
GCP	Good Clinical Practice
GMP	Good Manufacturing Practice
GXP	GCP+GLP+GMP
ICT	Information and Communication Technologies
IHE	Integrating the Healthcare Enterprise
IQ	Installation Qualification
KKS	Coordination Centre for Clinical Trials
KKSN	Network of Coordination Centres for Clinical Trials
MVP	Master validation Plan
ObTiMA	Ontology-based Trial Management Application
OQ	Operational Qualification
PACS	Picture archiving and communication system
PLM	Product Lifecycle Management
PQ	Performance Qualification
PIC/S	Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-operation Scheme
PLM	Product Life Cycle Management
QA	Quality assurance
QMS	Quality Management System
SaaS	Software as a Service
SAE	Severe Adverse Event
SDLC	Software Development Life Cycle
SLA	Service Level Agreement
SME	Small Medium Enterprises

SOA	Service Oriented Architecture
SOP	Standard Operating Procedure
SQA	Software Quality Assurance
STaRC	Study Trial and Research Centre
SUSAR	Suspected Unexpected Serious Adverse Reaction
SVMP	System Validation Master Plan
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TDD	Test Driven Design
URS	User Requirements Specification
VPH NoE	Virtual Physiological Human network of excellence
WP	Work Package
WT	Work plan Table

7.5 Questionnaires for Gap Analysis (Templates)

7.5.1 General and business requirements (to be answered by management)

7.5.1.1 General questions

Question	Comment
Tool name and version number	
Tool description	
Is the tool already be used (by whom, in how many studies)? How many subjects per study does the tool support?	

7.5.1.2 Module 1: Description of development environment

No.	Question	Answer (yes, no, not rel.)	Comment (if answer "yes", please specify)
1	What is the structure of the developer group (one place, distributed)?		
2	Number of developers?		
3	Are the responsibilities of each member in the group described?		
4	Prior projects in the field of medical research where developers participated?		
5	Is an organogram of the software development group available and current?		
6	Does the development group have sufficient qualified and experienced personnel in order to adequately perform the development of p-medicine software tools?		
7	Provides p-medicine the developers with sufficient resources?		
8	Does the p-medicine developer group agree with a developer audit/evaluation by ECRIN?		
9	Does p-medicine allow insight into the source code?		
10	Does p-medicine agree to an "escrow		

	agreement"?		

7.5.1.3 Module 2: Business model and maintenance

1	How is the sustainability of the product provision guaranteed by p-medicine?		
2	How will the p-medicine tool be provided to ECRIN and other users?		
3	Is there a business plan for the provision of the p-medicine tool available?		
4	What is the business model of p-medicine after the end of EU-funding (e.g. stability of financial background)?		
5	Does a Business continuity plan exist?		
6	Can tool developers / p-medicine group provide support for the software user?		
7	Can tool developers/ p-medicine group maintain services for the software user?		
8	Can tool developers/ p-medicine group provide user training?		
9	Does the unit have adequate staff to provide support / maintenance?		
10	Is there a plan for ongoing development of the tool?		

7.5.2 Questionnaire: Requirements for a CDMS system used for data collection in GCP compliant clinical trials

7.5.2.1 General aspects and system limitations

No	Requirement	Commentary (Yes, no, in development, n/a, specifics, description, …)
1	Is your system completely web-based? Completely web□based means that all modules (e.g. user administration, study setup and maintenance, data entry) can be configured and used with full functionality via a web browser).	
2	If no: please list the web-based modules and describe the functionality provided.	
3	Does your system allow conducting multiple studies at the same time (e.g. manage different user accounts across different studies)?	
5	Is there a limit to the number of studies that can be conducted simultaneously?	
6	Is there a limit to the number of patients that can participate in a study?	
7	Is there a limit to the number of users who can use the system (total or simultaneously)?	
9	Is there a limit to the number of validity rules that can be defined for a study?	
10	Is there a limit to the number of data fields per eCRF?	

7.5.2.2 Aspects data quality during data collection

18	Does your system support repeating data items (1 to n entries of element groups, e.g. concomitant medication, within a single form, an additional 'row' will be displayed when the last 'row' is filled in)?	
19	Does your system support repeating forms, meaning that the number of a form depends on the occurrence of an event (e.g. Adverse Event Form)?	
20	Does your system support repeating study events, meaning that the number of a “study event” depends on the occurrence of a previous event?	
21	Does your system support conditional forms, which are opened automatically in case a pre□defined condition is	

	met (e.g. an AE is categorized as SAE)?	
22	Does your system support the definition of data items or data item groups that become editable or visible only if a predefined condition is met?	
23	Is the creation of eCRFs graphically oriented (design by mouse), or tabular oriented (table of data items)? Exists the possibility for modification of eCRF after the creation of the eCRF?	
	Does the creation of eCRFs has different steps (e.g. draft, test, validation)?	
24	During designing the eCRF, is it possible to define a header for each form? Can the header contain: Text objects Dynamic objects (e.g. Subject ID)	
25	Is the versioning of eCRFs supported?	
26	Is it possible to establish a library with eCRF elements with: - CRF pages - CRF modules - variables - other objects	
27	CRFs can be assigned to a visit.	
	Sample collection can be assigned to a visit?	
28	Repeating visits are possible.	
29	Support of CDASH standard for data collection elements?	
30	Is the creation of CRFs for international trials supported? For example: - Multilingual CRFs - Multilingual help functions of eCRF - Consideration of different time zones, time specifications, etc. (MEZ, summer time, etc.)	

31	Consideration of different time zones (e.g. during data input or CRF update)?	
32	Lab data are shown in eCRF (e.g. as table)?	
33	Is there a limit to the number of parameters per eCRF, i.e. the number that can be collected and stored?	
34	Is there a limit to the number of studies that can be managed simultaneously?	
35	Is there a limit to the number of validity rules that can be defined for a study?	
36	Is there a limit to the number of users who can use the system (total or simultaneously)?	
37	Does your system allow the use of different date formats (e.g. for date German / US)?	
38	Does your system support the handling of incomplete date information?	
39	Does your system support derived data items, meaning that the value of these data items are calculated based on the values of other data items which are distributed over a set of forms / study events of the same subject?	
39	Is the change/update of eCRFs during study conduct based on an amendment of the study protocol possible and how can this be achieved in international trials?	
40	Does your system provide the possibility to deny registration of a subject if given conditions is not met?	
41	Can the following environments for data entry be established and managed within the application: - development - testing - training - production / operation	
42	Does your system offers integrated help functions? If yes: Is it possible to define study related help features e.g. tooltips for data items, context sensitive help?	
43	Is an automatic monitoring of input for consistency with a defined field type (e.g. data field) available?	

	- Use of parameter-related selection lists - Use of parameter-related value ranges - Use of standardised selection lists (e.g. diagnoses, medicines)	
47	Is the uniform use of international units (e.g. cm, inch) is supported?	
48	Which of the following supplementary functions for data monitoring and / or processing are available in the eCRFs of the software? - Spell checking of entered text - Automatic conversion of parameters (e.g. transformation of lab value unit into other unit) - Possibility of annotations at the document level - Display of protocol violations during data input	
49	Are the following options for data input supported in eCRFs? - Saving incomplete eCRFs - Saving invalid eCRFs - Collection and display of all error messages in list format after data input - Recording of errors - Others	

7.5.2.3 Training and support

50	Can support and training for CRA, investigator, data manager and data entry personal provided?	
51	Does a user support for forgotten pass words exist?	
52	Is a help desk for users provided?	
53	What is the average training requirement in employee-days for introduction to the software?	
54	Can you offer training for system administrators?	
55	Training for monitors is offered?	

56	Training for study managers is offered?	
57	Is additional training offered?	
58	Which of the following support and / or hotline services are you able to offer? - Hotline in German, other languages - Hotline in English - Telephone hotline - 24-hour hotline availability - Email hotline - Training by consultant - Training by p-medicine - Video courses	
59	Which forms of documentation do you provide for training - Printed documentation (manuals, etc.) - Media-based documentation (e.g. video) - Online documentation	
60	What type of support do you offer for eCRF design? - eCRFs can be prepared in collaboration with p-medicine - Collection of sample eCRFs is available - Training is provided by p-medicine	
61	What type of support do you offer for the installation of your software updates? - Technical support available for installation - Technical support available for update process - Update can be installed without additional aid from the company - Automatic update of the software	

	- Audit trail for upgrades is available - Test scripts for updates - Manual for updates	
62	What type of support do you offer for the expansion and programming of the software? - new interfaces created upon request - new functionalities created upon request - CDISC support	
63	Which of the following services do you offer? - Support for error correction in the software - Regular updates of the software - Regular meeting - User groups - Access to websites with news, problem-solving tips,…	

7.5.2.4 eCRF administration

64	eCRFs can be tracked/depicted/searched for according to: - patient - site - visit / time - investigator - country - total number of CRFs is shown	
65	In the eCRF incomplete eCRFs are indicated, flag lists of incomplete eCRFs can be generated	
66	The investigator should be able to sign an eCRF for approval? Can this eCRF approval function be modified for different countries?	

67	The system should support the import of lab data into the corresponding eCRF.	
68	Does your system support the management of laboratory reference ranges? If yes: Does your system provide the possibility to manage laboratory reference ranges per laboratory, including: - assignment of one or more laboratories to a site - possibilities for changes of site assignment during study execution	
69	Does the system support the definition of ranges for each laboratory parameter depending on laboratory, sex and age?	
70	Does your system provide a status for data items / forms / study events / subjects marking (e.g. data entry status, query status, SDV status, recruitment status)	
71	Does the system display graphic status icons for data items, forms, study events, subjects?	
72	Does your system support plausibility checks during data entry (“edit checks”)?	
73	Does your system support plausibility checks in batch mode (“batch checks”)?	

7.5.2.5 Audit trail and query system

	An Audit Trail records per item all: - data input actions - data changes (including value before and after change) - data deletions - date/time stamp and username of action - “Reason for change”	
	The “Reason for Change” of the audit trail is - always required - optional for defined variables - “change due to query”	

	- "Reason for Change" is logged	
	The characterisation as „Self Evident Corrections /Obvious Corrections" is possible	
	Is a query system for data cleaning available in the tool?	
	Queries can be listed according to: - patient - site/investigator - country - total number of queries	
	The creation of manual queries is possible; the creation of queries in batch modus is possible?	
	A query can be indicated as "resolved", when - Released by data manager - Released by monitor	
	Data query system: - Unequivocal query number is assigned - Specific query text is indicated - Query text can be modified	
	Identical queries are not generated during repeated query run in batch modus	
	Which options for eCRF validity checks does your software offer? - Setting mandatory fields - Definition of conditional branches (if-then rule) - Definition of validity checks for individual parameters - Definition of tests for logical consistency between parameters within documents (e.g. gender and pregnancy) - Definition of tests for logical consistency	

	between parameters of different documents (e.g. diagnosis and therapy)	
	Are unresolved queries flagged?	
	To the Investigator information that new queries exists is indicated: - when the investigator connects to the system - by e-mail	
	Does your system support the automatic generation of queries by checking for discrepancies?	
	Exists a link between the query and its discrepancy, so that a correction of the value will set the query status to “responded” or “corrected”?	
	Is it possible to link manually raised queries to a data item? Is it possible to link manually raised queries to a set of data items?	
	When resolving a query: is it possible to correct the value of a data item and to answer the query in a single step?	
	Does your system support query numbers (unique numbers for queries and query lists)?	
	Does your system provide the possibility to print a list of queries sorted site, country, subject, study event, related data items and date the queries were raised?	

7.5.2.6 Additional functions (data sharing / coding / analysis and reporting)

	Does your system support the transfer of a study subject with all data from one site to another site?	
	Does your system support data sharing with patient registers by providing an interface to integrate patient register data with clinical trial data?	
	Does your system provide the possibility to lock and unlock a study allowing only read access when locked?	
	Is it possible to input data from medical records into the eCRF? Can electronic source documents be used?	
	Is guaranteed that the sponsor does not have exclusive control of source documents and eCRF data?	

	Is a copy of the completed eCRFs (site specific patient data) stored independently from the study database at the corresponding site under control of the investigator?	
	Is it possible that in a clinical study the medical record may be the first place in which trial related data is recorded (source document) with later transfer of data to the eCRF?	
	Is a notification system integrated in your system that can trigger a notification of study related events (e.g. Adverse Event form, state of an eCRF "ready for review")?	
	Does your software offer the following options for the management of patient study data? - Issuing of an ID for study subject - Control of unequivocal assignment of ID - Customisation of patient IDs / study subject ID - Creating pseudonyms for subject IDs - Rendering primary data anonymous / pseudonymous - Storage of primary patient data in a separate database - Selection of patients according to personal data (age, gender, place of residence, etc.)	
	Which of the following parameters for the administration of eCRFs does your software utilise? - Date-, time stamp - Author logging - Indication of status parameters (e.g. cleaning status, Quality Assurance status, completeness) - Source data verification code for monitor	
	Which options does the software offer for status types of eCRFs (e.g. document stored, document incomplete, data erroneous, and document complete and checked)?	
	Is a fully automatic status checking supported? (e.g. automatic status checking with confirmation and user	

	modification options or status checking via manual user input)?	
	Does your system support the planning of monitoring visits?	
	Does your system support the conduct of source data verification (e.g. remote monitoring)?	
	Does your system support randomization?	
	Does your system provide an interface for the integration of randomization services?	
	Does your system support medical coding of terminology utilizing: - MedDRA - WHO Drug Dictionary - CTCAE (CTC) - ATC - ICD	
	Can your system manage different coding releases of the same coding dictionary?	
	Does your system manage different language versions of the same coding dictionary?	
	Does your system support auto□coding?	
	Are coding decisions recorded?	
	Does your system allow the printing of “annotated CRFs”? (The annotated CRF provides the variable name and the coding for each CRF item).	
	Does your system allow printing filled out / saved and empty eCRFs of a subject or a site?	
	Does the system generate reports? (e.g. query status report, database structure report, plausibility check report, audit trail reports, user reports).	
	Is it possible to sort or filter reports by e.g. site, subject, form, data item, and/or status?	
	Does your system allow the import of data?	

	Does your system support the following import formats: - CSV - XML - HL7 - LAB - other	
	Does your system provide the possibility to export study data and metadata (including the audit trail) for the purpose of migration, application, and analysis?	
	Is it possible to filter data for export?	
	Is your system CDISC certified for: - Import (Data) - Import (Metadata) - Export (Data) - Export (Metadata)	
	Reports can be generated for: - Edit checks - Derivations - Database plausibility/ integrity checks	
	Report can be printed or exported concerning: - visits - eCRFs items	
	Is Change Management of CRFs (Version Control) supported? (e.g. control if in different centres in different countries different versions of an eCRFs are used for data entry).	
	Does the system generate country-specific reports for international trials, e.g. data quality reports?	
	Which types of analyses does your study-related software offer: Are standardised analyses according to centre, time,	

	etc. (e.g. recruitment lists) possible? Is data quality analysis possible?	
	Is a free configuration of analyses by centres, period, patient parameters, etc. possible? - Single-variable analyses - Two-variable (two-dimensional) analyses	
	Are standard reports provided by the tool? - Interim reports - Billing reports - Recruitment reports - Insurance reports - Study progress reports / status reports	

7.5.2.7 Electronic documents

	Which of the following study related documents (eDocuments) can the software generate, show, reference and/or manage: - Patient identification - Patient consent declarations - Storage of emergency medicines - Documents for specimen processing - Patient-related info sheets - Documents for specimen storage - Patient-related labels - Notification of patients regarding an examination - Patient warning letters - Research schedules for test physicians - Documents for exam scheduling - Release tickets for patients - Scheduling for therapy	

	- Therapy-related documents - Scheduling / Planning of medicine(s) - Chemotherapy records - Radiotherapy records - Documents for medicine optimisation (e.g. dosage) - Documentation of toxicity criteria - Documents regarding parallel therapies - Incident reports - Patient-care documents - Examination results / reports - Physicians' letters - Others	
	Which of the following options does your software offer for the management of eDocuments? - Date-time stamp - Audit-trails / Author tracking - Setting of multiple status parameters - Version control	
	Which selection options are available for the access to eDocuments? - Selection according to various criteria (e.g. centre, addressee, date) - Direct retrieval by input of name or number - Restriction of accessibility according to the user's status and access rights	

7.5.2.8 Platform requirements

	The Platform on which the server runs is: - UNIX/Linux	

	- Windows Server - Other	
	The database system for the study database is: - Oracle - Microsoft SQL - PostgreSQL - Other	
	What web browsers can be used?	
	Is the data transfer encrypted?	
	Are specify browser features mandatory, like Flash or Java Script?	
	Which web server is used: - Microsoft - Apache - Tomcat - Other	
	Can the system be hosted? - Internally at ECRIN data centre - Externally by p-medicine - Externally by an independent hosting provider	
	Does your system offer a well-defined and stable application interface (API), which can support interoperability with other systems?	
	Does your system support the setup of an extended data protection scheme?	
	A step-by-step database lock is possible (e.g. soft lock): - per patient - per site - per eCRF	

	A step-by-step database unlock is possible: - per patient - per site - per eCRF	
	Any database lock or unlock is automatically recorded	
	Can a report about locked data be generated?	
	The complete database can be exported as: - XML - ODM - SDTM - Other format	
	Is it possible to export from study database only the eCRFs / collected study data per site?	
	Is study archiving supported? - Database export as ODM/XML - eCRFs export as PDF - References exist to documents that exists as paper documents (e.g. signed informed consent)	
	Is personal patient data separated from medical study data?	
	Is information available about system stability and system available during operation (e.g. Load test / Stress test) / Performance)?	
	Are trivial administration issues performed automatically; e.g. triggered by a user in case of a forgotten pass word?	
	Password and log-in features cover: - minimal password length - forced password change after 1st login - forced password change after defined time - defined complexity of password - recording of password history	

	- minimum of changed characters - restricted number of failed logins	
	Possible definition of user roles with assignment of specific rights possible for - Data Entry - Data Manager - Monitor - Investigator - Patient - System administrator - Other self-defined roles	
	Is the definition of User Groups with assignment of specific rights (e.g. study group) possible?	
	Are e-mails sent by the system in encrypted form?	
	Which of the following procedures are integrated into the software? - Encrypted sending of usernames and passwords - Encrypted saving and storage of data and documents - Backup-Restore system (e.g. secondary hard disk, DVD) - Crash protection (hard-disk imaging) - Loss of connection triggers automatic log-off	

7.5.2.9 Implementation support

	Is an Installation Guidance including scripts for installation provided?	
	Can the installation be performed by ECRIN data centre personal?	
	User manuals are provided for - Data managers - investigators - system administrators - monitors	

	- Others	
	Will p-medicine support installation of the system in an ECRIN centre?	
	Will p-medicine support system validation of the system in an ECRIN centre, by: - Providing validation documents (requirements, test results, QA documents) - Providing test scripts - Joint conduct of validation	
	Will p-medicine support maintenance of the system in an ECRIN centre?	

7.5.3 Requirements for imaging in GCP compliant clinical trials (assessment of Dr.Eye)

7.5.3.1 General aspects and system limitations

No	Requirement	Commentary (Yes, no, in development, not applicable, n/a, specifics, description, …)
1	What components of your imaging system are web□based modules (please describe the functionality provided).	
2	Does your system support image handling during the conduct of clinical trials?	
3	Does your system allow image handling during multiple trials at the same time (e.g. manage different user accounts across different trials)?	
4	Is there a limit to the number of trials that can be conducted simultaneously?	
5	Is there a limit to the number of images that is supported?	
6	Is there a limit to the number of users who can use the system (total or simultaneously)?	
7	Is there a limit in the size of the images?	
8	What are the components of your imaging system? - a picture archiving system (PACS), a web-based picture archive system - a connection to a clinical data management system (CDMS, EDC) - an imaging amendment tool - DICOM viewer - an image processing unit - a portal or web entrance (a single access unit for all study participants) - an image review unit - an image analysis unit	

	- an data extraction unit - an image transfer system - others	
	If your system has no PACS as a component, does your system interact with a PACS?	

7.5.3.2 Quality aspects of imaging in clinical trials

9	Does your system checks quality of incoming images?	
10	Does your system support the use of validated standardized image analysis techniques?	
11	Does your system support the standardized extraction of quantitative image information?	
12	Are validated and standardized image processing techniques used?	
13	Is the PACS system that is part of your tool marked as a medical product (CE certificate)?	
14	Is your tool marked as a medical product (CE certificate)?	
15	Is the loss-less transfer of information (imaging data) guaranteed?	
16	Does your system generate transfer protocols?	
17	Is a centralized analysis of imaging data supported?	
18	Are validated DICOM protocols used to ensure a lossless transfer of images via internet	
19	Is the upload of an image data set accompanied by a quality check that assures that the data set fulfils the trial rules, e.g. regarding patient anonymity of the image meta information	
20	Can the user define generic quality specifications, e.g. Base Clinical, Clinical CT, de-identification, etc.	
21	Are measures performed on the image bitmap itself, such as checking for burned-in identifying information, evaluating of contrast, or checking that the correct anatomy has been imaged?	

7.5.3.3 Process aspects of imaging and standards in clinical trials

22	Is the electronic transmission of imaging data between different sites and the central repository supported?	
23	The combined management of imaging and numerical and other data by linking image storage with the clinical data management system is supported	
24	Is high availability (site independent) and well-structured access to data, images and trial results provided?	
25	Is it possible to specify rules to be set up for individual studies, for example to ensure a consistent use of information in DICOM tags?	
26	Does your system support the definition of data items or data item groups that become editable or visible only if a predefined condition is met?	
27	Are numerical analysis results automatically exported into a CRF?	
28	Is it possible that the investigator can input own clinical trials images / clinical imaging data?	
29	Is it possible to send/receive images by the investigator from any personal computer?	
30	Does the imaging system exchange data with a data management system for clinical trials (e.g. import image number in CRF, link between CRF and image)?	
31	Is a central image repository for the clinical trial supported? Are local image repositories used?	
32	Are transfer, up-/down-load and viewing of imaging data via internet from a local personal computer to/from a central PACS possible?	
33	Is it possible to send/receive images by the investigator from the local PACS to be used by your tool?	
34	Is it possible to define parameter of the study protocol in your tool to support the workflow of image handling?	
35	Is it possible to clean data / correct/edit data? Is any correction/change of data accompanied by an audit trail?	
36	Does your tool support image post-processing and analysis? When yes, what kind of processing?	

37	Does your tool support the joint usage of CDMS/EDC, PACS and image processing tools?	
38	Allows your tool searches in the imaging data bases?	
39	Does your system generates reporting forms related to image acquisition and analysis (e.g. presence of image artefacts or patient compliance)	
40	Does your tool support DICOM and DICOM protocols? Is a DICOM dictionary included?	
41	Are analysis results of your tool send back to the PACS in the format of DICOM and DICOM Structured Reports.	
42	Can Image analysis results be queried and retrieved? Can they be queried through DICOM interface?	
43	Exists the option to call PACS and the image processing unit from the clinical data management system (e.g. EDC system) for cross-linking of data and for enabling semantic searches in the database?	
44	Can the following environments for image handling be established and managed within the application: - development - testing - validation - training - production / operation	
45	Can your tool provide imaging data with expert annotations?	
46	Can metadata be managed by the imaging tool?	
47	Can images be tracked/depicted/searched for according to: - patient / PID - site - visit / time - investigator - country	

	- total number of images uploaded is shown	
48	Are corrupted images flagged?	
49	Does your tool support imaging review, does it provide image approval functions during image review?	
50	Does your system assign a status to images (e.g. image reviewed, image analysed)? Does the system display graphic status icons for the images?	
	Can different types of images be handled (e.g. MRI, CT, PET, or ultrasound)?	
	Is it possible to integrate a third party for image evaluation / review?	
	Is it for an analysis core lab possible to log in, submit, and retrieve data / images?	
	Are open standards in accordance with the Integrating the Healthcare Enterprise (IHE) supported? Are established standards such as DICOM, HL7, and XDS supported?	
	Does your system support image retention? Do policies, especially security policies, exist?	
	Can the system generate automated alerts, e.g. for outliers or according to specified criteria? Are the alerts send via email, text, system messages?	
	Can the PACS or another database be used for long-term archiving of study images after the end of the study?	
	Is Source Data Management supported? Are the eSDI requirements / recommendations for managing electronic source data applied to imaging?	

7.5.3.4 Data security and data protection aspects

	Is the access to the data base /imaging repository controlled? Has each user of the tool to register a user account before using the system?	
	Can all privileges and access rights be controlled via user accounts, e.g. who is allowed to upload and download data/images, access certain images?	
	Is data protection (privacy) guaranteed? Are different national laws for Data Protection considered?	
	Does the system support following security relevant methods:	

	- https, secure web-protocol - eligibility check of users - each user has only access to assigned data - during the image up-load, all private header information will be automatically removed and replaced by a pseudonymous patient identifier (PID) - does your tool generate pseudonyms or does it interact with a tool to generate pseudonyms (e.g. PID generator) - imaging data is transferred through the internet only in pseudo-anonymous form - storage of all data/images is done pseudo-anonymously - it is possible to encrypt the pseudonym (PID) during transfer via internet and during storage - it is possible to integrate a TTP in the operations - the tool to generate pseudonyms (PID) will be located and operated by a trusted party (TTP)	
	Is image generation, transfer and storage tracked? Is a tracking report provided?	
	Is the access to the PACS subject to concepts of access rights (e.g. each research group / site has its own secured environment and the access to data is strictly regulated according to the specifications of each group)?	
	Does your system provide the possibility to deny registration of a subject if given conditions is not met?	

7.5.3.5 Training and support

	Can support and training for CRA, investigator, image reviewer, image analyser and data managers be provided?	
	Does a user support for forgotten passwords exist?	
	Is a help desk for users provided?	
	Does your system offer integrated help functions?	
	What is the average training requirement in employee-days for introduction to your tool?	

	Can you offer training for system administrators?	
	Which of the following support and / or hotline services are you able to offer? - Hotline in German, other languages - Hotline in English - Telephone hotline - 24-hour hotline availability - Email hotline - Training by consultant - Training by p-medicine - Online documentation	
	Which forms of documentation do you provide for training - Printed documentation (manuals, etc.) - Media-based documentation (e.g. video) - Online documentation	
	What type of support do you offer for the parameterisation of your tool / image analysis validation? - Image validation in collaboration with p-medicine - Image analysis in collaboration with p-medicine - Training provided by p-medicine	
	What type of support do you offer for the installation of software updates? - Technical support available for installation - Installation Guidance including scripts - Technical support available for update process - Update can be installed without additional aid from the company - Automatic update of the software	

	- Audit trail for upgrades is available - Test scripts for updates - Manual for updates	
	What type of support do you offer for the expansion and programming of the software? - new interfaces created upon request - new functionalities created upon request - new analysis algorithms - image analysis validation	
	User manuals / SOPs are provided for - Data managers - investigators - image reviewers - image analysts - system administrators - monitors - others	
	Will p-medicine support system validation of the imaging system in an ECRIN centre?	
	Will p-medicine support installation of the imaging system in an ECRIN centre?	
	Can you support an ECRIN centre, by: - Providing validation documents (requirements, test results, QA documents) - Providing test scripts - Providing image validation scripts - Joint conduct of validation	
	Will p-medicine support maintenance of the system in an ECRIN centre?	

7.5.3.6 Platform requirements

	What web browsers can be used?	
	Is the image data transfer encrypted?	
	Are specify browser features mandatory, like Flash or Java Script?	
	Can the system be hosted? - internally at ECRIN data centre - by p-medicine - externally by an independent hosting provider	
	Does your system offer a well-defined and stable application interface (API), which can support interoperability with other systems?	
	Password and log-in features cover: - minimal password length - forced password change after 1st login - forced password change after defined time - defined complexity of password - recording of password history - minimum of changed characters - restricted number of failed logins	
	Which of the following procedures are integrated into the software? - Encrypted sending of usernames and passwords - Encrypted saving and storage of data and images - Backup-Restore system (e.g. secondary hard disk, CD-ROM) - Crash protection (hard-disk imaging) - Loss of connection triggers automatic log-off □	

7.5.4 Requirements for a system to support biobanking in clinical trials (for assessment of Biosample Manager)

7.5.4.1 General management and study set-up

No	Requirement	Commentary (Yes, no, in development, n/a not applicable, specifics,…)
26	User, centres, institutions, can be created	
27	Biosampling is integrated with clinical data management system (e.g. EDC system)	
28	The input of biosamples information in eCRF is possible	
29	Institutions should be able to assign in the system centres (sites)	
30	The system must be able to capture automatically the current date and time.	
31	The system must be able to generate unique identifiers (pseudonyms) for patients.	
32	Samples should be managed, employing: - Centre details - Analysis / extraction lists - Addition of extraction - Deactivation of extractions - Destruction notification	
33	System should support study controlling processes: - Audit trail - Data history - Audit results - Notification list about process controlling - List of assigned centres - List of studies - List of study access	
	System should be possible to set up of a new	

	clinical study. In each study the number of collected samples as well as the complete storage time of samples is indicated.	
34	System should be able to consider sites of a trial, containing information about: - leading investigator - study number - study start - study end - participating countries - participating sites - date of last update - site ID - telephone number - number of enrolled patients - date of first patient, first visit - date of last patient, last visit	
35	Management of centres (sites) should be possible containing information about: - number of participating sites - number of planned patient recruitment - status of study - number of collected samples - storage duration of samples - location of samples	
36	Management of central sample repository (CSR). It should be possible to assign each CSR an own admin role with following data: - name - role	

	- collaborator ID / employee ID - telephone number - mail address - authorisation date	
37	Set up of new institutions, labs or clinics must be possible. A list per institution with assigned centres can be generated.	
38	Each CSR can have assigned any number of study sites	
39	Each institute can be set up with following data: - name of institute - type - name of responsible person - address - country - telephone - mail - authorisation date	

7.5.4.2 Sample acquisition /check in requirements

No	Requirement	Commentary (Yes, no, in development, n/a not applicable, specifics,…)
41	Sample Acquisition: The system must allow users to upload and associate signed informed patient consent forms with biological sample records.	
42	The system should have a link/reference to the patient informed consent	
43	The system should support the creation of informed patient consent form templates which: - are in a language understandable to the subject or their representative - list the research projects for which the biological samples given by the subject will be used - address the future use of the samples (including commercial use and unspecified use) - provide information about the release of individual research results	

	- provide information about consent withdrawal or later modification	
44	The system must support the withdrawal of patient consent by the patient or their legal representative	
45	The system must allow authorized users to alter the scope of patient consents according to the patient's or their legal representative's requests.	
46	The system must allow authorized users to enter new biological sample records.	
47	In addition to compulsory sample data, the system should allow users to enter the following data when importing biological samples: - identifier - depositor's name and address - source, substrate or host from which the biological material was isolated - geographical origin of material - growth media and conditions, cell preservation or storage conditions where known; - hazard information, e.g. in the form of a safety data sheet.	
48	The system should be able to store the shipping records (shipping log) which document biological sample arrival	
49	The system must support the anonymization of samples in the following ways: - removal of identifying data - two-way coding by double pseudonymisation.	
50	The system should support the review of the anonymization. It should allow a suitably authorized user to confirm the anonymisation procedure.	
51	The process of anonymization and its review must be logged by the system	
52	Generation of a pseudonym for a barcode (BC1)should be possible	
53	The system should be possible to generate a second pseudonym for a second barcode (BC2)	
54	The system should manage the check-in of patients, including following information: - informed consent is available - BC1 search - BC1 as well as BC2 is checked for validity - following information is checked: date of visit in centre, type of sample (blood, serum, tissue, others... - sex of patient - BC1 and BC2	

55	Creation of a new trial; system should guarantee that for each study the number of samples to be taken out of the storage as well as the complete storage time is indicated. Following steps should be managed: - Pseudonymisation of barcode 1 - check-in of patient - check: informed consent is available - BC1 search - BC1 as well as BC2 is checked for validity	
56	It should be possible to check-in patients	
57	System must guarantee that samples of studies are coded threefold: 1. Study participant number (patient number) 2. First pseudonym (BC1, barcode 1) 3. Second pseudonym (BC2, barcode 2). The sample is stored only with BC2.	
58	After the check-in of new samples: BC2 is generated BC2 replaces BC1	
59	Generation of an unequivocal patient number: every patient study ID is used only once in the system, this is checked when a new ID is assigned	
60	Check-in of patients without IC entry should be possible	
61	It should be guaranteed that every sample can be identified only by its BC2 (second pseudonym)	
62	The system can generate an inventory list of all samples collected for a study, in a country, per site or patient.	
63	There should be no limit on the number of BC codes possible	
64	The system should be able to read BCs	
65	The system should make it possible that a patients withdraws from a study, inclusive the deletion of patient number and corresponding samples	
	The system should allow the change of centres	
	The system should allow a patient audit	
	BC2 should have a length of at least 14 characters	
	Pseudonymisation BC2: the system checks that BC2 has been assigned to a sample before the sample is being stores in the biobank	

	During patient check-in the system checks the validity of the informed consent	
	System may request informed consent information	
	During patient check-in the system checks that all patients of a study have been assigned to a site	
	The system supports the pseudonymisation of patient's informed consent A patient's informed consent can be deposited in the system	
	Pseudonymisation of BC1 scan; it is guaranteed that the assigned BC is not used again in the study	
	BC1 verification: a scanned BC is checked according to given validity criteria	
	A patient identification number (study-ID) is generated; an already assigned study ID can be imported	
	The system allows double input of patient study numbers to avoid typing errors.	
	The system must be able to track the physical location of samples by allowing users to associate the following data with samples: - location - container	
	If the sample container's metadata include information about the container's location, the system is not required to store the location of the sample separately.	
	The system must allow users to track the movement of samples by recording the following data: - current location - a predefined number of previous locations - date moved from last location - date received at current location - person responsible for the move	
	The system should support the validation of biological samples by allowing users to record details of the validation process, including the following data: - location of the validation - list of items validated - customer name and address - date of receipt of items to validate - date of validation - type of action carried out on the sample (e.g. purity check, quality check, identity check) - reference to sample plans and procedures where relevant - validation results with units of measurement - any abnormalities observed	

	- person responsible for the validation results	

7.5.4.3 Selection / Requests for samples / Retrieval

	A process for request and selection of samples should be possible	
	Sample request should be possible. Upon request a list with following information is generated: - study - CSR - number of samples - name of analysis / extraction - due date	
	After sample request, a list is generated covering all samples of the request with following information: - SGN - BC2 - material - amount - units used - status of sample - status of process	
	For a request a list with selected BC2s is send to the sample manager The sample manager finds and checks out the requested samples from the biobank	
	Request of sample status should be possible. Samples with following status are depicted, but not selected: - destruction requested - destroyed - lost - empty - shipped	
	Request for sample selection. Right samples are selected on the basis of BC2 and made available	
	The trustee should be able to search for patients, but only for patient number or BC1	
	The system should support sample retrieval. It should track all requests for sample retrieval. This includes recording the following data: - date of request - list of samples requested - person who requested samples (investigator) - purpose of retrieval (study)	
	The system should allow authorized users to approve, partially approve or reject sample requests.	

7.5.4.4 General system requirements and interoperability

	An interface with a biobank management system should be supported	
	What steps of biosampling is supported by your tool, what by the biobank?	
	It should be possible to create new users Only the administrator can activate and deactivate users	
	Only the administrator can assign following roles: 1. Clinic (site): data manager, process controller, auditor 2. Lab: administrator, sample registrar, sample manager	
	The system can create a list of all users	
	The Trustee can make changes in the system concerning the informed consent of patient, only when patient expresses wishes to change in written form	
	Only process controller and auditor can see all processes in the system, about a study, or about a single sample	
	The system must allow authorized users to export - sample records, and - a catalogue of sample records	
	The system should log all export operations.	
	The system should be able to import - sample records, and - records of other entity types - imported records are subject to data validation	
	The system should use an open or a well-document proprietary data interchange format to support the interaction of the system with external software products	
	The system should support a graphical user interface.	
	The system can display text elements of the user interface (e.g. button text, tool tips, error messages) in the local language. The system should be able to display the text elements of the user interface in English	
	The system must be documented in sufficient detail: - functions - fields in data entry forms - errors and possible solutions	
	The system must provide online help: - context sensitive;	

	- provide visual guidance	
	The system should assist data entry by following measures: - suggest possible text values - drop down menus when possible - provide default values	
	The system should be possible to generate error messages or alerts	
	Error messages produced by the system must be meaningful, so that users can decide how to correct the error or cancel the process.	
	System recovery must be possible	
	The system must provide an automatic backup feature	
	The system must provide a recovery feature for restoring entities from backup files.	
	The capability of data backup by the system must be checked regularly	

7.5.4.5 Security issues

	The system must record the following data per log: - action - entities involved - user undertaking action - date and time of action	
	The system must record automatically all critical actions in an log: - actions which result in the deletion of entities - anonymization / pseudonymisation - data modifications - user management actions - user authentication attempts - access violation attempts - changes to log settings	
	The system must not allow users to access the tool without authentication	
	The system must support authentication by user ID and password.	
	The system must ensure that the data entered by the user during authentication cannot be intercepted by third parties	
	The system must log both successful and unsuccessful user authentication attempts.	
	If the system receives an unsuccessful user authentication attempt, the system must not reveal any information about the validity of the user ID.	

	If the system registers more than a predefined number of consecutive unsuccessful user authentication attempts from the same IP address, the system may refuse to accept further attempts from that address	
	The system should not allow users to have unsecure passwords, i.e. character strings which: - are less than 8 characters long - can be found in dictionaries - are not made up of a combination of letters, numbers and punctuation marks - are on a list of prohibited character strings (e.g. “password”, “123456”)	
	To protect health information of patients, the system adheres to privacy laws with respect to information systems.	
	The logistics for a withdrawal of consent must be clearly defined and conveyed to all subjects at the time of consent.	
	Anonymization should be verified by an appropriate review procedure.	
	The system must support the management of information related to the following sample lifecycle processes: - sample acquisition, including sample collection and receipt of samples - storage of samples and associated data - processing of samples - disposition, selection, retrieval of samples	
	The system must not allow users to associate identifying data with non-identifiable biological samples	
	The system guarantees that no role except „sample registrar“ or „code exchanger“ has access to patient number or BC1	
	The system should be able to send and receive encrypted messages.	
	The system should store passwords and similar credentials in an encrypted form.	
	The system should store protected health information	

	and users' personal data in an encrypted form.	
	The system must test whether the input value matches the format specified for the given field	
	The system must ensure that the input value satisfies metadata constraints (e.g. age).	
	The system must check the spelling of text field inputs.	
	The system should allow authorized users (users have the required permission) to access: - sample records - procedure records - documents (e.g. informed consent) - storage unit records - user records	

7.5.5 Questionnaire for requirements regarding tool development and quality management (to be answered by developers and quality managers)

7.5.5.1 Overview over the developer group

Question	Comment
Description of developer group	
Composition of group, number of developers, number of supporting staff	
Lead of developer group (name)	
Organisation/Institution	
Experience	
Prior projects	

7.5.5.2 Software development planning, code writing and use of standards

No.	Question	Answer (yes, no, not rel.)	Comment (if answer "yes", please specify)
1	How is software development planned and conducted?		
2	Is a conventional or agile approach used for software development?		
3	In case of an agile approach, how is it organized (product owner, scrum master, meetings)?		
4	Does a software development plan (SDP) exist?		
5	Do developers participate in training?		
6	Are members of the software group trained to perform their development activities?		
7	Do SOPs for the development activities exist?		
8	Are the activities for managing the requirements reviewed by management?		
9	Does an information security policy exist?		
10	Do information security awareness, education and training exist?		
11	Do developers have knowledge/experience with testing and validation of computer systems (e.g.		

	previous audits, inspections)?		
12	Are there reports of previous audits or inspections available?		
13	Are developers familiar with the regulatory background for software for clinical research (e.g. GCP)?		
14	Are developers familiar with the evaluation of patient risks during development planning?		
15	Is software developed /maintained/adapted according to SDLC (Systems development life-cycle)?		
16	Are there programming standards available for each programming language that is used?		
17	Is good technical documentation for the tool available?		
18	Do the standards cover the following details - Naming conventions for files - Naming conventions for variables - Log-out conventions - Versioning (which tools), including documentation history - Error handling - Rules for writing code - Rules for lines with comments - Conventions concerning platform - Conventions concerning user interface		
19	Is the compliance with development standards and data standards assessed?		
20	Do you support the CDISC standard?		
21	Do you support ISO2701?		
22	Are written policies in place and employed for document review?		
23	Is there a unique definition, which documents underlie a review process?		
24	How is the review process organized?		
25	Are processes for deviations specified?		
26	Is system documentation that covers system architecture, individual modules / classes and their inputs, outputs, and purposes developed that can be provided?		
27	Is “In line Commenting” employed?		
28	Does a reference installation for the p-medicine tool exist?		
29	Does the reference installation represent a functionally equivalent testing environment?		
30	Does a demo installation of the p-medicine tool for ECRIN user training exist?		
31	Can the reference installation be used for testing configuration changes?		

32	Can the reference installation be used by ECRIN users for the assessment of the tool?		
33	Does the reference installation consists of separate phases: e.g. initial installation, then test phase use and routine use?		
34	Are written policies in place and employed for integrity tests, security checks, patches and updates that are security relevant?		
35	Are written policies in place for emergency precautions?		

7.5.5.3 Quality management during development

No	Question	Answer (yes, no, not rel.)	Comment (If answer "yes", please specify)
1	What is your quality management system (QMS)? Do you have a quality manager?		
2	What Software Quality Assurance (SQA) activities exist in your group? Do you have a Quality Handbook?		
3	The Software Quality Assurance (SQA) activities are reviewed with management on a periodic basis		
4	Are software quality assurance activities trained?		
5	Does SQA review the activities and development products of the group?		
6	Follows the group a written policy for managing requirements?		
7	Follows the group a written policy for managing the software project?		
8	Follows the group a written policy for software configuration management?		
9	Follows the group a written policy for employing and maintaining a standard software development process?		
10	Follows the group a written policy for training?		
11	Can written policies be provided for a developer audit by ECRIN?		
12	Are adequate resources provided for quality management activities?		
13	Are adequate resources provided for tracking reviewing the software project progress?		
14	Are adequate resources provided for the software development process?		
15	Are adequate resources provided for training and dissemination of tool usage?		

16	Does the quality management system include a quality plan for the p-medicine project, covering: - Roles and responsibilities - Documentation standards - Measures of quality assurance - Tools, methods and standards for development - Code review - Traceability		
17	Are written instructions (e.g. SOPs) employed for: - Software development - Change control - Configuration management - Review and approval of documents - Support of software problems - Supervision of project plans - Storing and archiving of quality relevant documents - Archiving of software (source code) - Management of problems - User access and physical/logical security - Handling of complaints - Performance of audits by customers?		
18	Are there standards for the technical and user documentation (e.g. user manual)?		
19	What Quality Control Activities are performed? For example: - Check for transcription errors in data input and reference - Check the integrity of database - Check for consistency of data - Check for uncertainties in data, database files, etc - Review of internal documentation - Check methodological and data changes resulting in recalculations - Undertake completeness checks - Compare new results to previous results		
20	How does the group perform the testing of the software tools?		
21	Is testing done by a dedicated and independent person/group?		
22	Are written policies in place and employed for the test activities?		
23	Do you perform: - Functional tests - Non-functional tests - Acceptance tests - Regression tests - System tests - Software tests - Integration tests		

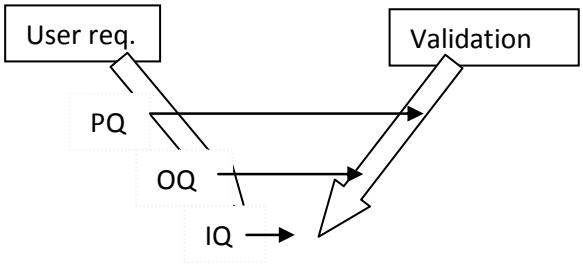
	- Unit tests - Database tests		
24	Do you conduct risk-based testing? (Risk based testing uses risk to prioritize the appropriate test cases)		
25	Do you test according to risks of GCP relevance (e.g. risks for patient's wellbeing)?		
26	Do the standards cover the following details - Naming conventions for files - Naming conventions for variables - others		
27	Is the compliance with standards assessed?		
28	Are there standards used for planning, performing and reporting of tests?		
29	Exists a Software Quality Control / Testing Plan and how is it implemented?		
30	Is the testing done in a systematic way?		
31	Does separation of development, test and operational activities exist?		
32	Are the tests structured with respect to different phases? Is it possible to differentiate and allocate the tests (white-box testing, black-box testing, user acceptance testing)?		
33	Does the test plan cover the following points - System characterization, incl. status of development - Objectives of testing/relationship to risk analysis - Test cases - Test data, including acceptance criteria - Performance, amount of testing - Results of tests, including descriptions of deviations - Assessment of results, if applicable changes dependent on the development phase (SDLC) and repeated testing? - others		
34	Is there a systematic approach to the specification of the amount of testing?		
35	Are the evaluators/reviewers different persons than the developers?		
36	Are test tools used?		
37	Is there a documented procedure for change control for the: - SDLC - Source code - Hardware specification and operational qualification - Configuration data		

38	Is there a clear definition, from which change on a re-testing, completely or partly, is necessary?		
39	Are responsibilities for change management defined (release of change, implementer, reviewer)?		
40	Are there procedures to prevent that an update or change of a software module is performed undetected or simultaneously by several persons?		
41	Is assured that after changes to the system have been done, tests (preferably the same tests, regression tests) have to be performed?		
42	Is it possible to audit changes from the proposal to the implementation?		
43	Is it possible to uniquely identify each version of each configuration element?		
44	Are delivered versions of hard- and software systems, including documentation, somehow archived?		

7.5.5.4 Generic requirements for GCP compliance of the tool

No.	Requirements for GCP compliance	Answer (yes, no, not rel.)	Comment (if answer "yes", please specify)
1	Plays GCP compliance aspects during the planning of the programming of p-medicine tools a role?		
2	Is all clinical trial information be recorded, handled, and stored in a way that allows for accurate reporting, interpretation and verification?		
3	Is the confidentiality of records that could identify subjects protected, respecting the privacy and confidentiality rules in accordance with the applicable regulatory requirements?		
4	Are the tools implemented with procedures that assure quality? Can evidence for quality implementation be provided?		
5	Allows the tool that the investigator can ensure the accuracy, completeness, legibility, and timeliness of the data reported in the CRFs (or other records)?		
6	Supports the tool that data reported in the CRF that are derived from source documents, are consistent with the source documents?		
7	Supports the tool that any change or correction to a CRF is being dated, initialled, and explained (if necessary); is an audit trail maintained?		
8	Does the tool support that all data are generated, documented (recorded), and reported in compliance		

	with the protocol, GCP, and the applicable regulatory requirements?		
9	Does the tool ensure that the electronic data processing system conforms to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance: is the tool validated?		
10	Are SOPs (standard operating procedures) for using the tool (system) available and maintained?		
11	Is the tool designed to permit data changes in such a way that the data changes are documented and that there is no deletion of entered data (i.e. audit trail, data trail, edit trail)?		
12	Is a security system maintained that prevents unauthorized access to the data?		
13	Is a list maintained of the individuals who are authorized to make data changes?		
14	Is adequate backup of the data maintained?		
15	Exist safeguards for the blinding (e.g. maintain the blinding during data entry and processing, pseudonyms)?		
16	Is it possible to always be able to compare the original data and observations with the processed data in the system (tool)?		
17	Is the use of an unambiguous subject identification code supported that allows identification of all the data reported for each subject?		
18	Allows the tool direct access to source data/documents for trial-related monitoring, audits, IRB/IEC review, and regulatory inspection?		
19	Can requirements documentation (e.g. functional requirements) be provided to support system validation?		
20	Can test documentation be provided to support system validation?		
21	Can test reports be provided to support system validation?		
22	Are test reviews, including document reviews, performed in the different phases of tool development (e.g. unit tests, integration tests, IQ, OQ, PQ)?		
23	Does the developer or another p-medicine group perform system validation of the developed software?		
24	Do test reports exist that can become part of the		

	validation plan?		
25	Does the developer or another p-medicine group support the user conduct of IQ, OQ, PQ?		
	Explanation: Validation process  		System validation process and user requirements IQ=installation qualification OQ=operational qualification PQ=performance qualification
26	How is data security in your tools guaranteed?		
27	Does protection against malicious and mobile code exist?		
28	Is information back-up implemented?		
29	Does an access control policy exist?		
30	Does user access management and user registration exist?		
31	Does a policy for user password management exist?		
32	Does secure log-on procedure exist?		
33	Does a procedure for user identification and authentication exist?		
34	Does a password management system exist?		
35	Is the sensitive part of the system isolated from the other parts?		
36	Does a validation procedure for the input of data exist?		
37	Does a policy for the use of cryptographic controls exist?		
38	Does access control to source code exist?		
39	Does a control of technical vulnerabilities exist?		
40	Is risk management applied throughout the lifecycle of the computerized system (taking into account patient safety, data integrity and product quality)?		
	Are decisions on the extent of validation/verification and data integrity controls based on a justified and documented risk assessment of the system?		
	Can close cooperation between all relevant personnel such as Process Owner, System Owner, Developers, Qualified Persons and IT personal be		

	shown?		
	Do all personnel have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties?		
	Is it assured that the competence and reliability of a developer/supplier are key factors when selecting a product or service provider?		
	Is it assured that quality system and audit information relating to supplier or developers of software and implemented systems are being made available to inspectors/auditors on request?		
	Can developers justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment?		
	Does a listing of all relevant components of the developed tool and their GXP functionality exist?		
	Does for critical tools a written description of the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures exist?		
	Do Requirements Specifications describe the required functions of the tool and are they based on a risk assessment of GXP impact.		
	Are user requirements traceable throughout the life-cycle of the tool?		
	Is it ensured that the tool has been developed in accordance with an appropriate quality management system?		
	Is the customized computerised system/tool formally assessed and are quality and performance measures for all the life-cycle stages of the system reported?		
	Is evidence of appropriate test methods and test scenarios demonstrated? Are particularly, system (process) parameter limits, data limits and error handling considered?		
	If data are transferred to another data format or system, are validation checks conducted that data are not altered in value and/or meaning during this migration process?		
	Do computerised systems/tools exchanging data electronically with other systems/tools have appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize risks?		
	For critical data entered manually, does an additional check on the accuracy of the data exist?		
	Does risk management of the tool development exist and does it cover the criticality and the		

	potential consequences of erroneous or incorrectly entered data?		
	Is data secured by both physical and electronic means against damage?		
	If data is stored by the tool, is stored data checked for accessibility, readability and accuracy? Can the access to data be ensured throughout the storage period?		
	Are regular back-ups of all relevant data conducted?		
	Is the integrity and accuracy of back-up data and the ability to restore the data checked?		
	Is it possible to obtain clear printed copies of electronically stored data?		
	Is it possible to generate printouts indicating if any of the data has been changed since the original data entry?		
	Is it considered during development that, based on a risk assessment, the creation of a record of all GXP-relevant changes and deletions (a system generated "audit trail") is built into the system?		
	Are audit trails available and convertible to a generally intelligible form and regularly reviewed?		
	Are any changes to a computerised system/tool including system configurations only possible in a controlled manner in accordance with a defined procedure?		
	Are physical and/or logical controls in place to restrict access to computerised system/tool to only authorised persons?		
	Does the extent of security controls depend on the criticality of the computerised system/tool?		
	Are the creation, change, and cancellation of the access authorizations recorded?		
	Do the management systems for data and for documents record the identity of operators entering, changing, confirming or deleting data including date and time?		
	Are all problems, system failures and data errors reported and assessed?		
	Are electronic records, when used for clinical trials, signed electronically (e.g. by password)?		
	Does the electronic signature has the same impact as a hand-written signature; is it permanently linked to its record, and includes the time and date that it was applied?		
	Are provisions in place to ensure continuity of support for critical processes (e.g. data entry) in the event of a system breakdown?		

	If relevant changes are made to the system, is the ability to retrieve all data ensured and tested?		

7.5.6 Assessment sheet for risk analysis of deficiencies in the business plan

Risk Analysis: Business plan							
Risk Analysis	**Description/cause**	**Prob.**	**Impact on tool provision**	**Impact on p-medicine**	**mitigation measures (preventive measures)**	**contingency measures (what to do if risky situation occurred)**	**responsible team/person**
developer unit	A well structured developer group does not exist	low	high	high	management takes care of groups	new personal is employed	USAAR
developer unit	The developer group is not well organised						
developer unit	No sufficient number of developers, and supporting staff is available						
developer unit	Are the responsibilities of each member in the group described?						
developer unit	What are the experiences of the member of the developer group?						
developer unit	no participation of developers in prior relevant projects in the field can be demonstated						
developer unit	no organogram of the software development group is available and current						
developer unit	developer group has not sufficient qualified and experienced personnel						
developer unit	sufficient resources are not provided to p-medicine the developers						
developer unit	developer group do not agree to a developer audit/assessment						
business plan	no insight into the source code by the tool user is possible						

business plan	p-medicine does not agree to an "escrow agreement"						
business plan	P-medicine cannot guarantee the sustainability of the product provision						
business plan	p-medicine fails to be able to provide the tool users/customers						
business plan	p-medicine tools are not maintained over a long periode after						
business plan	No plan for the continous updated of p-medicine tools exist						
business plan	no robust business plan for the provision of p-medicine tool exist						
business plan	No realistic business model for p-medicine exists after the end of EU-funding (considering e.g. stability of financial						
business plan	No Business Continuity Plan exist						
business plan	Tool developers / p-medicine group are not able to provide support efficiently						
business plan	Tool developers / p-medicine group are not able to maintain tools/services						
business plan	Tool developers / p-medicine group cannot provide user training efficiently						
business plan	p-medicine units do not have adequate staff to provide support / maintenance efficiently						
business plan	There no plan for ongoing development of the tool after EU funding ends						

7.5.7 Assessment sheet for risk analysis of deficiencies in GCP compliance

7.5.7.1 Risk analysis of ObTiMA

(As example ObTiMA is used, but this sheet was not completed in time for the deliverable; it can be used for all tools)

Risk Analysis: OBTIMA							
Risk Analysis	**Description/cause**	**Prob.**	**Impact on single tool**	**Impact on p-med.**	**mitigation measures (preventive**	**contingency measures (what to do if risk occurred)**	**responsible team/person**
GCP compliance aspects	GCP compliance aspects are not considered during software planning and programming of ObTiMA	low	high	high	GCP training for developers and QA managers	developber audit	ObTiMA
clinical data security	clinical are not recorded, handled, and stored in a way that allows for accurate reporting, interpretation and verification						
confidentiality of records	confidentiality of records that could identify patients is not protected, respecting privacy and confidentiality						
Quality assurance	ObTiMA is not implemented with procedures that assure data quality						
data quality	ObTiMA does not enable the investigator to ensure accuracy, completeness, legibility, and timeliness of the data recorded						
consistency with source documentation	data reported in the CRF fail to be consistent with the source documents/data						
audit trail	ObTiMA doesn't maintain a stable audit trail for data collection						
validation	ObTiMA fails to be validated for GCP compliance						

SOPs	SOPs (standard operating procedures) for using the tool are missing						
data audit trail	Obtima does not document all data changes and allows the deletion of entered data						
missing authorisation	no list is maintained for individuals who are authorized to use ObTiMA and enter data						
lacking traceability of data	tool is not able to compare the original data and observations with the processed data in the system						
erroreous trial subject identification	ObTiMA fails to use an unambiguous subject identification code						
developer assessment	p-medicine cannot produce requirements documentation (e.g. functional requirements) for system validation						
developer assessment	p-medicine cannot produce test documentation (report, scripts) for system validation						
developer assessment	p-medicine group cannot support the user during IQ, OQ, PQ						
system security	no protection against malicious and mobile code exist						
system security	no access control policy exist						
system security	a policy for user password management is missing						
system security	the sensitive part of the system is not isolated from the other parts						
system security	the input of data is not validated						
data security	no access control to source code exists						

developer assessment	technical vulnerabilities of the system are not controlled						
developer assessment	risk management is not applied throughout the lifecycle of ObTiMA						
developer assessment	documented risk assessment is not used to decide about necessary validation and data integrity controls in ObTiMA						
developer assessment	lack of cooperation between Process Owner, System Owner, Developers, Qualified Persons and IT personal						
developer assessment	p-medicine personnel does not have appropriate qualifications and defined responsibilities						
developer assessment	p-medicine is not able to provide quality system and audit information from developers of software for inspections						
Quality assurance	developers are not able to justify their acceptance criteria, procedures and records based on their risk assessment						
validation	no listing of all relevant components of ObTiMA and their GXP						
validation	ObTiMA requirements specifications do not describe the required functions and are not based on a risk assessment of GXP impact						
validation	user requirements of ObTiMA are not traceable throughout the life-cycle of the tool						

validation	ObTiMA was not developed in accordance with an appropriate quality management system						
validation	Quality and performance measures of ObTiMA are not reported for all the life-cycle stages of the system						
Quality assurance	evidence of appropriate test methods and test scenarios cannot be demonstrated (e.g. system parameter limits, data limits and error handling)						
data quality	after data is beeing transferred to another data format or system, no validation checks are conducted						
data quality	ObTiMA does not contain appropriate built-in checks for the correct and secure entry and processing of data						
data quality	stored data cannot be accessed, read and is not accurate						
data quality	after a period data cannot be accessed						
data quality	after a back-up data cannot be correctly restored						
data quality	it is not possible to print copies of electronically stored data						
data quality	it is not possible to get printouts indicating changes of data since the original data entry						

system security	the extent of security controls depend not on the criticality of the computerised system or tool						
system security	no record exist abozt the creation, change, and cancellation of the access authorizations						
system security	the identity of users entering, changing, confirming or deleting data including date and time is not always recorded						
system security	not all problems, system failures and data errors are reported and assessed						
system security	ObTiMA cannot attach an electronic signauture (e.g. by password) to records used in clinical trials						
system security	The electronic signature is not permanently linked to its record, and does not includes the time and date that it was applied						
system security	p-medicine cannot ensure continuity of support for critical processes (e.g. data entry) in the event of a system breakdown						
system security	after changes are made to the system, all data cannot be retrieved completely						

7.5.7.2 Risk analysis of Portal

Risk Analysis: Portal							
Risk Analysis	Description/cause	Probability	Impact on single tool	Impact on p-medicine	mitigation measures (preventive measures)	contingency measures (what to do if risky situation occurred)	responsible team/person
The host server crashes	The portal server crashes because of hardware problems	medium	high	high	(a) Regular back-up of the portal instance, configuration files and the portal database; (b) Having a ready for usage backup server	(a) Setup a new server and make sure that it properly works and fix the primary server in the meantime; (b) make sure the back-up server runs and that it properly works and fix the primary server in the meantime	IBMT
Accessing the portal is not possible	The portal instance is not accessible because after after a power breakdown not all services have been automatically started	medium	high	high	Regularly check skripts for starting the portal instance and related Data Mining services automatically	Start the portal instance and related Data Mining services manually; check skripts for automatically starting.	IBMT
Single Sign-On is not possible	After logging in in the portal a user have to login in a p-medicine tool (e.g. ObTiMA) again	medium	high	high	Configuring user credentials in the p-medicine tools correctly	Example ObTiMA: make sure that the user id is correctly entered in the ObTiMA database; check Single Sign-On again	p-medicine tool developers, e.g. UdS
Login in the portal is not possible	Login in the portal is not possible because of hardware problems on the Identity Provider server	medium	high	high	Having a ready for usage backup server	Make sure the back-up server runs and that it properly works and fix the primary server in the	CUSTODIX
Login in the portal is not possible	Login in the portal is not possible because the Identity Provider server is not running	medium	high	high	Having a messaging system for getting information if the server is not running	Restart the Identity Provider server and make sure that it properly works	CUSTODIX
Creating an account in the portal is not possible	A new user enters a wrong e-mail address on a registration form and never receives a confirmation e-mail for activating his account	low	low	low	(a) the user has to enter his e-mail address two times; (b) the user will see the entered e-mail address again for checking it; (c) the user will be informed about a time limit for waiting for the confirmation e-mail; (d) providing a global p-medicine support email address in the portal.	After expiration of the time limit for waiting for receiving a confirmation e-mail, the user can contact an admin or e.g. mail a global p-medicine support email address	IBMT; CUSTODIX
GCP compliance aspects	GCP compliance aspects are not considered during software planning and programming of the Portal	high	low	high	Developers of p-medicine tools and services integrated in the portal take care for GCP compliancy of the tools before integrating them in the portal	Before a p-medicine tool tool is integrated in the portal, the portal administrator should clarify with the developers of the tool if it is GCP conform. A desicion about an integration of a toll should be discussed with project leader.	All developers of p-medicine tools and services integrated in the portal
clinical data security	clinical data are not recorded, handled, and stored in a way that allows for accurate reporting, interpretation and verification						
confidentiality of records	confidentiality of records/data that could identify patients is not protected, respecting privacy and confidentiality						

Quality assurance	Portal is not implemented with procedures that assure data quality						
data quality	Portal does not enable the investigator to ensure accuracy, completeness, legibility, and timeliness of the data recorded						
validation	Portal fails to be validated for GCP compliance	medium	high	high	Regularly check scripts for starting the portal instance and related Data Mining services automatically	Start the portal instance and related Data Mining services manually; check scripts for automatically starting.	IBMT
SOPs	SOPs (standard operating procedures) for using the tool are missing						
missing authorisation	no list is maintained for individuals who are authorized to use the Portal and enter data	low	low	low	The users' roles and rights concept provided by the framework and supported by the p-medicine securiry framework excludes missing authorisation for executing different tasks in the portal	The portal administrator checks roles and rights assigned to the portal users and edits them if necessary	IBMT, CUSTODIX
erroreous trial subject identification	the Portal fails to use an unambiguous subject identification code						
developer assessment	p-medicine cannot produce requirements documentation (e.g. functional requirements) for system validation						
developer assessment	p-medicine cannot produce test documentation (report, scripts) for system validation						
developer assessment	p-medicine group cannot support the user during IQ, OQ, PQ						
system security	no protection against malicious and mobile code exist						
system security	no access control policy exist	low	low	low	User roles and rights concept provided by Liferay framework and extended by security layer in p-medicine supports an access control to resources integrated in the portal	The portal administrator checks the portal log files. If the control policy doesn't work, the portal administrator communicates with developers of the security framework of p-medicine	IBMT, CUSTODIX
system security	a policy for user password management is missing	low	low	low	The first page shown for a portal user during his first login in the portal should provide the policy for user password management.	The portal administrator should edit the web page shown on the first page for a portal user during his first login in the portal. The project members responsible for legal framework should discuss the content of the policy.	IBMT, UdS, LUH

system security	the sensitive part of the system is not isolated from the other parts	low	low	low	The sensitive part of the portal is a management of user credentials is stored within the security infrastructure by CUSTODIX. It is fully separated from the non-sensitive parts stored on the portal server hosted by IBMT.	The portal administrator contacts the responsible person for the security framework in order to solve the occurred problem.	IBMT, CUSTODIX
system security	the input of data is not validated	low	low	low	The input of data in the portal is validated by Liferay framework, which is used for p-medicine. The input of data on the registration and login pages provided by CUSTODIX is also validated in the source code integrated in the portal by CUSTODIX. Developers of p-medicine tools and services should include validation into the source code of a developed tool before its integration in the portal.	The portal administrator will discuss with developers of the p-medicine security solution and with developers of p-medicine tools about implementing of validation for the fields for input data, if necessary.	IBMT, CUSTODIX, all developers of p-medicine tools and services integrated in the portal
data security	no access control to source code exists	low	low	low	The portal source code and the source code for all integrated p-medicine tools is hosted by IBMT on the server secured with password. No ssh connection to the server for non-authorized users is allowed. Access to the server is logged in log files of the server.	The portal administrator checks the log files for accessing the server. The access credentials will be changed if necessary: periodically AND if there are entries about an unauthorized access in the server log files.	IBMT
developer assessment	technical vulnerabilities of the system/ the portal are not controlled	low	low	low	In order to avoid vulnerabilities of the portal the following steps should be performed: - The access to the portal uses a connection (ssl); -running of the Tomcat server used for the portal is performed by non-root user; -Tomcat user will not have remote access to the server; - auto-deployment of web applications will be disabled; - the Tomcat configuration and the file permissions on the Tomcat folder should be changed for avoiding changes in the Tomcat configuration, deploy new web applications or modify existing web applications; The portal administrator should regularly check if new information about vulnerabilities is available on the official web page of the Liferay project (http://www.liferay.com/de/community/security-team/known-vulnerabilities) and perform necessary steps for avoiding these issues	The portal administrator should check on the official web page of the Liferay project (http://www.liferay.com /de/community/security-team/known-vulnerabilities) if the occures vulnerabilities are already solved and if yes, he should perform necessary steps for avoiding these issues. If not: he should inform the Liferay developers about a new issue.	IBMT, Custodix
developer assessment	risk management is not applied throughout the lifecycle of the Portal						
developer assessment	documented risk assessment is not used to decide about necessary validation and data integrity controls in the Portal						

developer assessment	lack of cooperation between Process Owner, System Owner, Developers, Qualified Persons and IT personal	low	low	low	Developers of the p-medicine services and tools permanently communicate with the portal administrator in order to achive standardized integration of the tools in the p-medicine evironment	Developers of the p-medicine services and tools should cooperate more if nesessary	IBMT, CUSTODIX, all developers of p-medicine tools and services integrated in the portal
developer assessment	p-medicine personnel does not have appropriate qualifications and defined responsibilities	medium	medium	medium	Qualification of developres of tools and services should allow to develop software for integrating them in the portal	Developers of tolls should provide robust, mature and secure software for integrating them in the portal	IBMT, CUSTODIX, all developers of p-medicine tools and services integrated in the portal
developer assessment	p-medicine is not able to provide quality system and audit information from developers of software for inspections	medium	medium	medium	Software for tools and services are available on the portal server and could be provided for inspection by request	Developers of tools should include audit information in the software necessary for inspections	All developers of p-medicine tools and services integrated in the portal
Quality assurance	developers are not able to justify their acceptance criteria, procedures and records based on their risk assessment						
validation	no listing of all relevant components of the Portal and their GXP functionalities exist	medium	medium	medium	Description of the portal components is currently available in the Deliverable D8.2	Description of the portal components should be provided on the project Wiki and should be continously updated if	IBMT, CUSTODIX, all developers of p-medicine tools and services
validation	the Portal requirements specifications do not describe the required functions and are not based on a risk assessment of GXP impact	medium	medium	medium	Requirements for the p-medicine portal are available in DoW and an Deliverable D8.2	Requirements specification for the p-medicine portal based on risk assesment should be provided on the project Wiki	IBMT
validation	user requirements of the Portal are not traceable throughout the life-cycle of the tool	medium	medium	medium	User requirements of the p-medicine portal are available in DoW and an Deliverable D8.2	User requirements of the p-medicine portal should be traceable throughout the life-cycle of the project	IBMT
validation	The Portal was not developed in accordance with an appropriate quality management system						
validation	Quality and performance measures of the Portal are not reported for all the life-cycle stages of the system						
Quality assurance	evidence of appropriate test methods and test scenarios cannot be demonstrated (e.g. system parameter limits, data limits and error handling)						
data quality	after data is beeing transferred to another data format or system, no validation checks are conducted						
data quality	the Portal does not contain appropriate built-in checks for the correct and secure entry and processing of data						
data quality	stored data cannot be accessed, read and is not accurate						

data quality	after a period data cannot be accessed						
data quality	after a back-up data cannot be correctly restored	medium	medium	high	Backup of the portal database and directories with important data (configurations, settings, workflows for data mining tool) as well as files for deployment of p-medicine tools is available on the project server in IBMT.	Backup should be done more often in order to retrieve more data while restoring	IBMT
system security	the extent of security controls depend not on the criticality of the computerised system or tool						
system security	no record exist abozt the creation, change, and cancellation of the access authorizations	low	low	low	Information about creation, change, and cancellation of the access authorizations is available in log files on the portal server hosted in IBMT and on the identity provider server hosted in CUSTODIX Logging of	Maintenance of the portal server and servers of the security infrastructure should contain back-up of records in log files	IBMT, CUSTODIX
system security	the identity of users entering, changing, confirming or deleting data including date and time is not always recorded	low	low	low	the identity of users accessing the portal is managed in the portal and in the projects security infrastructure. Using the p-medicine services and tools integrated in the portal is recorded in log files on the portal server. Processing of data (changing, confirming or deleting) occurs inside of the tools integrated in the portal.	The portal administrator and persons responsible for secure access to the portal should check if the identity of users accessing the portal is always recorded. Developers of tools integrated in the portal should check if records for changing, confirming and deleting data is available in their tools and provide this functionality if necessary.	IBMT, CUSTODIX, all developers of p-medicine tools and services integrated in the portal
system security	not all problems, system failures and data errors are reported and assessed	medium	medium	medium	The portal administrator checks the log files on the portal server and solves the problems. If the problems consern the tools integrates in the portal, he discusses the issues with the responsible tool developers.	The portal administrator should check the the log files on the portal server more often in order to provide promptly fixing of occured problems.	IBMT, CUSTODIX, all developers of p-medicine tools and services integrated in the portal
system security	p-medicine cannot ensure continuity of support for critical processes (e.g. data entry) in the event of a system breakdown	high	high	high	A ready for usage backup server should be started immediately. Data entry should be repeated by users	The portal administrator should install the backup server, update it if nesesssary and check ist functioning regularly	IBMT
system security	after changes are made to the system, data cannot be retrieved completely	medium	medium	medium	The roles and rights concept of the portal enables access of authorized users to resources in the portal. The portal administrator manages permissions of users to the resources.	The portal administrator checks if permissions of users to the portal resources are correct and edits them if necessary	IBMT