Deliverable No. 11.1

Evaluation and validation criteria for clinical adaptation

Grant Agreement No.:	600841
Deliverable No.:	D11.1
Deliverable Name:	Evaluation and validation criteria for clinical adaptation
Contractual Submission Date:	31/03/2014
Actual Submission Date:	02/06/2014

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

COVER AND CONTROL PAGE OF DOCUMENT	
Project Acronym:	**CHIC**
Project Full Name:	Computational Horizons In Cancer (CHIC): Developing Meta- and Hyper-Multiscale Models and Repositories for In Silico Oncology
Deliverable No.:	D11.1
Document name:	Evaluation and validation criteria for clinical adaptation
Nature (R, P, D, O)[1]	R
Dissemination Level (PU, PP, RE, CO)[2]	PU
Version:	0.1
Actual Submission Date:	02/06/2014
Editor: Institution: E-Mail:	Norbert Graf USAAR graf@uks.eu

ABSTRACT:

This deliverable presents in concrete details, tailored as groundbreaking check-lists, the advanced set of guidelines, evaluation and validation requirements to support all project partners as well as the external evaluators to standardize the clinical adaptation and validation process of CHIC platform tools, functionalities and frames with special focus on clinical and translational scenarios.

KEYWORD LIST:

Evaluation, validation, criteria, clinical adaptation, check-list, requirements

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 600841.

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

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

MODIFICATION CONTROL			
Version	**Date**	**Status**	**Author**
0.1	01/05/2014	Draft	Norbert Graf, USAAR
0.2	19/05/2014	Draft	Norbert Graf, USAAR
1.0	02/06/2014	Final version	Norbert Graf, USAAR

List of contributors

- Ruslan David, USAAR
- Fay Misichroni, ICCS-NTUA
- Dimitra Dionysiou, ICCS-NTUA
- Georgios Stamatakos, ICCS-NTUAA

Contents

1 Executive Summary

The CHIC project aims at developing cutting edge ICT tools, services and secure infrastructure to foster the development of elaborate and reusable integrative models (hypermodels) and large repositories so as to demonstrate benefits of having both the multiscale data and the corresponding models readily available. Although the broader VPH domain and *in silico* medicine are the primary targets of the hypermodelling infrastructure to be developed by CHIC, the primary application domain will be cancer and *in silico* oncology.

In the mid and long term CHIC aims to pave the way for reliable in silico clinical trials, lying at the heart of the vision of *in silico* medicine, and subsequently for patient individualized treatment optimization based on *in silico* experimentation.

According to the different goals and requirements of this project specified in detail in the different workpackages (WPs) and tasks, a clinical adaptation and validation process within the project will be carried as a major part of quality control and guarantee for further usage of tools and models, including the Oncosimulator. The spectrum ranges from testing of tools and models up to their usage in clinical trials. Hence, WP11 will identify objectives that need to be specifically tested in each case. For that reason proper evaluation criteria will be defined. This WP is crucial in that it will continuously assess the quality of all services and tasks of the CHIC environment and iteratively give feedback to all responsible persons.

This report presents the set of guidelines and check-lists to support evaluators to standardize the clinical adaptation and validation process including standardized reports. Such reports will suggest possible improvements, modifications and other functionalities to the technical WPs in a feedback loop.

Considering the user needs as described in WP2 and the aim for developing hypermodels based on scenarios within an infrastructure compliant with legal and ethical requirements, this document defines evaluation and validation criteria and identifies specific application objectives to be tested during the validation process.

Procedures in monitoring the development of hypermodels according to the defined evaluation and validation criteria are elaborated and criteria for their execution by specific user groups are presented. The work and related activities from other EU research projects have been considered and cited.

2 Activities and Tasks

2.1 Validation Criteria

Tools and models validation activities could be performed similarly to the medical software validation process which is accomplished through a series of tasks that are planned and executed at various stages of the software development life cycle. These validation criteria related tasks are adapted from the Food and Drug Administration (FDA)'s General Principles of Software Validation publication[3] and aligned to CHIC project's tasks and activities.

2.1.1 Tools and Models Life Cycle Activities

For integrative model (hypermodel) development the developers should establish a software life cycle strategy that is appropriate for their product and organization. The selected tool/software life cycle should cover the tool/software from its birth to its retirement. Activities in a typical software life cycle model include the following:

- Quality Planning
- System Requirements Definition and Specification
- Design
- Construction or Coding
- Testing
- Installation
- Operation and Support
- Maintenance
- Retirement

Verification, testing, and other tasks that support software validation have to be implemented during each of the above activities. A life cycle process organizes these software development activities in various ways and provides a framework for monitoring and controlling the software development project. Several software life cycle models (e.g., waterfall, spiral, rapid prototyping, incremental development, etc.) are well known by CHIC project partners.

For each of the software life cycle activities, there are certain "typical" tasks that support the conclusion that the software is validated. However, the specific tasks to be performed, their order of performance, and the iteration and timing of their performance will be dictated by the specific software life cycle model that is selected and the safety risk associated with the software application. For very low risk applications, certain tasks may not be needed at all. However, the software developer should at least consider each of these tasks and should define and document in the related deliverables which tasks are or are not appropriate for their specific application.

The chapters bellow are generic and are not intended to prescribe any particular tool and model (hypermodel) life cycle description or any particular order in which tasks are to be performed.

[3] General Principles of Software Validation, Guidance for Industry and FDA Staff. Source: http://www.fda.gov/RegulatoryInformation/Guidances/ucm126954.htm [May 2014]

2.1.2 Quality Planning

Design and development planning should culminate in a plan that identifies necessary tasks, procedures for anomaly reporting and resolution, necessary resources, and management review requirements, including formal design reviews. A software life cycle model and associated activities should be identified, as well as those tasks necessary for each software life cycle activity. The plan should include:

- The specific tasks for each life cycle activity;
- Enumeration of important quality factors (e.g., reliability, maintainability, and usability);
- Methods and procedures for each task;
- Task acceptance criteria;
- Criteria for defining and documenting outputs in terms that will allow evaluation of their conformance to input requirements;
- Inputs for each task;
- Outputs from each task;
- Roles, resources, and responsibilities for each task;
- Risks and assumptions; and
- Documentation of user needs.

2.1.3 System Requirements Definition and Specification

Requirements development includes the identification, analysis, and documentation of information about the device and its intended use. Areas of special importance include allocation of system functions to hardware/software, operating conditions, user characteristics, potential hazards, and anticipated tasks. In addition, the requirements should state clearly the intended use of the software.

WP2 of CHIC project is elaborating and presenting the user needs and requirements for the proposed technological and clinical research infrastructure so as to develop an environment that is able to run hypermodels composed of existing and newly developed models by different end users (e.g. clinicians, researchers) with the goal to drive common clinical practice to preventive, predictive and participatory medicine. This is done by providing the clinical perspective of the project and by taking into account the state of the art, the state of research and the state of practice in the healthcare domains addressed by the project. This WP addresses the needs for developing secure and consistent hypermodels and the technological requirements (in conjunction with all other WPs) from a clinical application standpoint facilitating VPH research. The project consortium is taking into account the existing infrastructures already developed for VPH like the p-medicine and the VPH-share infrastructure dealing with heterogeneous data and models. As requirements are changing during the evolution of the project, the specification of user needs and requirements are continuously updated and documented in the frames of WP2.

2.1.4 Design

The software design specification is a description of what the software should do and how it should do it. Due to the complexity of the project and in order to enable persons with varying levels of technical responsibilities to clearly understand design information, the design specification may

contain both a high level summary of the design and detailed design information. The complete software design specification constrains the programmer/coder to stay within the intent of the agreed upon requirements and design. A complete software design specification will relieve the programmer from the need to make ad hoc design decisions.

The software design specification should include:

- Software requirements specification, including predetermined criteria for acceptance of the software;
- Software risk analysis;
- Development procedures and coding guidelines (or other programming procedures);
- Systems documentation (e.g., a narrative or a context diagram) that describes the systems context in which the program is intended to function, including the relationship of hardware, software, and the physical environment;
- Hardware to be used;
- Parameters to be measured or recorded;
- Logical structure (including control logic) and logical processing steps (e.g., algorithms);
- Data structures and data flow diagrams;
- Definitions of variables (control and data) and description of where they are used;
- Error, alarm, and warning messages;
- Supporting software (e.g., operating systems, drivers, other application software);
- Communication links (links among internal modules of the software, links with the supporting software, links with the hardware, and links with the user);
- Security measures (both physical and logical security); and
- Any additional constraints not identified in the above elements.

CHIC's WP6 named 'Cancer Models and Hypermodel Design' has the objectives to:

- develop clinically driven multiscale cancer models
- use these models along with already existing ones in order to produce elementary models (hypomodels or component models) of fundamental biological processes (biomechanisms)
- standardize the latter according to the guidelines to be provided by WP7.
- Subsequently produce hypermodels (integrated models) as demonstrators of the VPH hypermodelling methodology in the cancer domain
- test and validate all models.

2.1.5 Construction or Coding

Models and Hypermodels may be constructed either by coding (i.e., programming) or by assembling together previously coded components (e.g., from code libraries, off-the-shelf software, etc.) for use in a new application. Coding is the software activity where the detailed design specification is implemented as source code. Coding is the lowest level of abstraction for the software development

process. It is the last stage in decomposition of the software requirements where module specifications are translated into a programming language.

Coding usually involves the use of a high-level programming language, but may also entail the use of assembly language (or microcode) for time-critical operations. The source code may be either compiled or interpreted for use on a target hardware platform. Decisions on the selection of programming languages and software build tools (assemblers, linkers, and compilers) should include consideration of the impact on subsequent quality evaluation tasks (e.g., availability of debugging and testing tools for the chosen language). Some compilers offer optional levels and commands for error checking to assist in debugging the code. Different levels of error checking may be used throughout the coding process, and warnings or other messages from the compiler may or may not be recorded. However, at the end of the coding and debugging process, the most rigorous level of error checking is normally used to document what compilation errors still remain in the software. If the most rigorous level of error checking is not used for final translation of the source code, then justification for use of the less rigorous translation error checking should be documented. Also, for the final compilation, there should be documentation of the compilation process and its outcome, including any warnings or other messages from the compiler and their resolution, or justification for the decision to leave issues unresolved.

Source code should be evaluated to verify its compliance with specified coding guidelines. Such guidelines should include coding conventions regarding clarity, style, complexity management, and commenting. Code comments should provide useful and descriptive information for a module, including expected inputs and outputs, variables referenced, expected data types, and operations to be performed. Source code should also be evaluated to verify its compliance with the corresponding detailed design specification. Modules ready for integration and test should have documentation of compliance with coding guidelines and any other applicable quality policies and procedures.

Source code evaluations are often implemented as code inspections and code walkthroughs. Such static analyses provide a very effective means to detect errors before execution of the code. They allow for examination of each error in isolation and can also help in focusing later dynamic testing of the software. Documentation of the procedures used and the results of source code evaluations should be maintained as part of design verification.

2.1.6 Testing by the Developer

Software testing entails running software products under known conditions with defined inputs and documented outcomes that can be compared to their predefined expectations. It is a time consuming, difficult, and imperfect activity. As such, it requires early planning in order to be effective and efficient.

Test plans and test cases should be created as early in the software development process as feasible. They should identify the schedules, environments, resources (personnel, tools, etc.), methodologies, cases (inputs, procedures, outputs, expected results), documentation, and reporting criteria. The magnitude of effort to be applied throughout the testing process can be linked to complexity, criticality, reliability, and/or safety issues (e.g., requiring functions or modules that produce critical outcomes to be challenged with intensive testing of their fault tolerance features). Descriptions of categories of software and software testing effort appear in the literature, for example IEEE Computer Society Press, Handbook of Software Reliability Engineering.

2.1.7 User Site Testing

Testing at the end-user site is an essential part of software validation. The Quality System regulation requires installation and inspection procedures (including testing where appropriate) as well as documentation of inspection and testing to demonstrate proper installation.

Terms such as beta test, site validation, user acceptance test, installation verification, and installation testing have all been used to describe user site testing. For purposes of this document, the term "user site testing" encompasses all of these and any other testing that takes place outside of the developer's controlled environment. This testing should take place at a user's site with the actual hardware and software that will be part of the installed system configuration. The testing is accomplished through either actual or simulated use of the software being tested within the context in which it is intended to function.

User site testing should follow a pre-defined written plan with a formal summary of testing and a record of formal acceptance. Documented evidence of all testing procedures, test input data, and test results should be retained.

3 General Validation Check-List

The general validation check-list has been elaborated in direct linkage with the requirements and functionalities mentioned in the Annex 11 of the EudraLex, The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practice, Medicinal Products for Human and Veterinary Use.[4]

This annex applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together fulfill certain functionalities.

Requirement	*Met by*
	General
Risk Management	Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.
Personnel	There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.
Suppliers and Service Providers	When third parties (e.g. suppliers, service providers) are used e.g. 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.
	Project Phase
Validation	• **The validation documentation and reports should cover the relevant steps of the lifecycle.** Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment. • Validation documentation should include change control records (if applicable) and reports on any deviations observed during the

[4] Annex 11, EudraLex, The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practice, Medicinal Products for Human and Veterinary Use. Source: http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf [May 2014]

	validation process. • An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. • For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available. • User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle. • The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately. • For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system. • Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy. • If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.
Operational Phase	
Data	Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.
Accuracy Checks	• Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period. • Regular back-ups of all relevant data should be done. Integrity and accuracy of back-up data and the ability to rest or the data should be checked during validation and monitored periodically.
Printouts	• It should be possible to obtain clear printed copies of electronically stored data. • For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.
Audit Trails	Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.
Change and	Any changes to a computerised system including system configurations

Configuration Management	should only be made in a controlled manner in accordance with a defined procedure.
Periodic evaluation	Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.
Security	• Physical and/or logical controls should be in place to restrict access to computerized system to authorised persons. 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. • The extent of security controls depends on the criticality of the computerised system. • Creation, change, and cancellation of access authorisations should be recorded. • Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.
Incident Management	All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.
Electronic Signature	Electronic records may be signed electronically. Electronic signatures are expected to: • have the same impact as hand-written signatures within the boundaries of the company, • be permanently linked to their respective record, • include the time and date that they were applied.
Batch release	When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.
Business Continuity	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 (e.g. a manual or 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.
Archiving	Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.

4 Clinical and Translational Science Scenarios Validation

The objectives of WP3 are to validate the CHIC environment by focusing mainly on three different cancer types. The selected diseases are Wilms tumor, glioblastoma multiforme (GBM) and non small cell lung cancer (NSCLC).

These particular diseases are selected to address different aspects of the project. For all three cancer types, clinical relevant cases are defined. Data from these cases will be stored within the infrastructure of CHIC in a secure and anonymized way according to the legal and ethical framework of CHIC. The data from these concrete clinical scenarios will undergo processing within the environment, and validation of the environment will be based on the clinical and oncologic data produced by the same scenarios.

One of the common requirements for all clinical scenarios is to have in place the CHIC Portal with its related functionalities and frames.

Key Requirement	*Met by*
CHIC portal and user registration frames	The interfaces which allow a user to access a CHIC services. Users registering on the CHIC framework can be subdivided into two or three main classes: consortium users, external users and possibly patients
CHIC identity provider (IDP)	The IDP shows an authentication form in which a user can enter its username and password
CHIC Trusted Third Party (TTP)	De-Identification and Upload of data into the CHIC platform
Models and Hypermodels	Access to reusable integrative models (hypermodels) and larger repositories
Sematic annotation	The presence of semantic annotation frames
Data flow and integration	Data flow and data integration interfaces according to specific data types.

4.1 Wilms Tumor Scenario

SIOP trials and studies for Wilms tumor are running since the 1970s in Europe. More than 8000 children with Wilms tumor participated in these trials. These trials are always randomized prospective and multicentre trials.

Today they are GCP-conform and running in Europe, Brazil and other centres around the world under the umbrella of the International Society of Paediatric Oncology (SIOP). Retrospective data from former trials and prospective data from the current SIOP-2001 trial will be used for evaluation and validation of newly developed and validated models and hypermodels of CHIC.

In up to 100 patients with nephroblastoma, transcriptome analysis of the tumour will be done to get new insights in the biology of nephroblastoma. This data will be used for the development of a system biology model, which will form the basis of the bottom-up approach of the in silico model for nephroblastoma and thus improving the accuracy of the developed in silico Hyper-Multiscale Models.

ObTiMA will be used to serve as a Clinical Data Management System (CDMS) for the SIOP-2001. Heterogeneous data from ObTiMA, clinical data from syndrome diagnostics, imaging data from MRI, molecular data from serum (autoantibodies, miRNA, proteomics data, whole genome sequencing), as well as data from the planned and realized treatment schedule will be put together for evaluation and validation of the Meta- and Hyper-Multiscale Models and Repositories using existing models from VPH. Data sets will also be used for the integrated Oncosimulator and will be subsequently validated via clinical and oncologic outcome.

The data will provide help to design individualized treatment strategies in future, thereby avoiding unnecessary (long-term) side effects from chemotherapy and radiotherapy.

4.1.1 Validation Check-List

Requirement	*Met by*
Scenario description	D2.2 - Scenario based user needs and requirements (Chapter 5. Scenarios for Nephroblastoma): • Clinical scenario • Imaging scenario • Molecular scenario • Validation scenario • Machine learning scenario • Advanced Nephroblastoma scenario • Drug selection scenario
Available data	The availability of retrospective and prospective data: • Clinical data • Pathological data • Imaging data • Molecular data
Hypermodel	The hypermodel for nephroblastoma will predict the tumor volume shrinkage of nephroblastoma in single patients that are treated with preoperative chemotherapy.
Validation Protocol	Validation protocols for the end-users and developers will be continuously updated and the results will be collected in the frames of the tasks bellow. Task 12.3: Training activities (M12-48) SubTask 12.3.a: Workshops/Summer schools In order to train potential users on the use of the CHIC platform and get feedback from them from early on in the project's lifetime, a series of workshops/summer schools will be organised starting after the end of the first year until the end of the project with a minimum of three events organised (MS31, MS32, MS33). The validation protocol could be based on the attached Evaluation and Validation Protocol Template, Version 0.1 (Appendix 4).
Usage Survey	Questionnaire for usage of models and hypermodels in the clinical setting (Appendix 3) is elaborated and the data collection has been initiated. The collected results will be reported in the frames of the training events and to CHIC platform developers.

4.2 Glioblastoma Multiforme Scenario

Patients with malignant glioma have a dismal prognosis despite neurosurgery, radiotherapy and chemotherapy. The median survival after diagnosis is only 15 months. At time of relapse, the median survival is 6 months, and all patients are dead within 18 months. Although the disease belongs to orphan diseases, with an incidence of 3/100000/year, the community burden and the loss of years of life is highest amongst all types of cancers.

Immunotherapy is a fast developing fourth treatment modality for patients with malignant glioma. The treatment aims to stimulate the body's own immune defence in order to control the disease. Worldwide, several groups reported interesting clinical data with long-term survivors in small series of patients.

In up to 100 patients with glioblastoma, transcriptome analysis of the tumour will be done to get new insights in the biology of glioblastoma. This data will be used for the development of a system biology model for glioblastoma together with the available immunological data to form the basis of the bottom-up approach of the in silico model for glioblastoma and thus improving the accuracy of the developed in silico Hyper-Multiscale Models.

4.2.1 Validation Check-List

Requirement	*Met by*
Scenario description	D2.2 - Scenario based user needs and requirements (Chapter 6. Scenarios for Glioblastoma): • Clinical scenario • Imaging scenario • Molecular scenario • Radio- and chemotherapy scenario • Immunotherapy scenario • Validation scenario • Machine learning scenario
Available data	The availability of retrospective and prospective data: • Clinical data • Pathological data (Tumor characteristics) • Imaging data • Data inherent to the HGG-2010 protocol outline • Monitoring data • Molecular data
Hypermodel	The hypermodel for GBM will predict if a single patient, with specific pretreatment, surgical and tumor characteristics will benefit from adding DC vaccination to standard therapy, in terms of PFS at 6 months.
Validation Protocol	Validation protocols for the end-users and developers will be continuously updated and the results will be collected in the frames of the tasks bellow. Task 12.3: Training activities (M12-48) SubTask 12.3.a: Workshops/Summer schools In order to train potential users on the use of the CHIC platform and get feedback from them from early on in the project's lifetime, a series of workshops/summer schools will be organised starting after the end of the first year until the end of the project with a minimum of three events organised (MS31, MS32, MS33).

	The validation protocol could be based on the attached Evaluation and Validation Protocol Template, Version 0.1 (Appendix 4).
Usage Survey	Questionnaire for usage of models and hypermodels in the clinical setting (Appendix 3) is elaborated and the data collection has been initiated. The collected results will be reported in the frames of the training events and to CHIC platform developers.

4.3 Non-Small Cell Lung Cancer Scenario

Lung cancer is the leading cause of cancer for women and men. Non-small cell lung cancer (NSCLC) accounts for more than 80% of all lung cancer cases with the majority of cases detected in advanced stages that do not allow curative surgery. Due to limited success of systemic chemotherapies up to now, the 5-Year Survival Rate amounts to 15%.

New molecular-based "personalized" therapies focus on inhibition of signal transduction pathways i.e. the EGFR pathway, the VEGF pathway, the RAS-, RAF- und EML4 pathway. After selection according to sequencing data or DNA FISH, the first trials could be finished showing the effectiveness of these drugs after molecular tests from tumor tissue after sequential molecular testing for second or third line therapies.

In the near future, it will be necessary to know the tumor-specific pathways very early after tumor diagnosis to choose the most promising therapy as first line therapy, maintenance or adjuvant therapy. For that purpose a system biology model will be developed based on the transcriptome analysis of up to 100 tumour specimen to get new insights in the biology of NSCLC. This data will form the basis for the bottom-up approach of the in silico model for NSCLC and thus improving the accuracy of the developed in silico Hyper-Multiscale Models.

4.3.1 Validation Check-List

Requirement	*Met by*
Scenario description	D2.2 - Scenario based user needs and requirements (Chapter 7. Scenarios for Non-Small-Cell Lung Cancer (NSCLC)): • Clinical scenario • Imaging scenario • Molecular scenario • Drug selection scenario • Validation scenario • Machine learning scenario
Available data	The availability of retrospective and prospective data: • Clinical data • Pathological data (Tumor characteristics) • Imaging data • Molecular data • Data inherent to the HGG-2010 protocol outline • Monitoring data • Molecular data
Hypermodel	The NSCLC hypermodel will focus on the both most frequent types of adenocarcinoma of the lung: the adenocarcinoma with predominant acinar pattern and the adenocarcinoma with predominant solid pattern. Various basic clusters of processes (biomechanisms) will be modelled at the cell/

	tissue level in appropriate hypomodels.
Validation Protocol	Validation protocols for the end-users and developers will be continuously updated and the results will be collected in the frames of the tasks bellow. Task 12.3: Training activities (M12-48) SubTask 12.3.a: Workshops/Summer schools In order to train potential users on the use of the CHIC platform and get feedback from them from early on in the project's lifetime, a series of workshops/summer schools will be organised starting after the end of the first year until the end of the project with a minimum of three events organised (MS31, MS32, MS33). The validation protocol could be based on the attached Evaluation and Validation Protocol Template, Version 0.1 (Appendix 4).
Usage Survey	Questionnaire for usage of models and hypermodels in the clinical setting (Appendix 3) is elaborated and the data collection has been initiated. The collected results will be reported in the frames of the training events and to CHIC platform developers.

4.4 Other Cancer Types Scenario

Tumors share many common features but also present striking differences, e.g. different cancer staging reflects their different ability to colonize the host and to induce angiogenesis and distant metastasis. These differences also have an impact on their natural history and the different clinical approach by which they are treated. In this task we will focus primarily on prostate cancer.

4.4.1 Validation Check-List

Requirement	*Met by*
Scenario description	D2.2 - Scenario based user needs and requirements (Chapter 8. Scenarios for prostate cancer): • Clinical scenario • Imaging scenario • Molecular scenario • Drug selection scenario • Validation scenario • Machine learning scenario
Available data	The availability of retrospective and prospective data: • EUREKA-1 Data • EUREKA-2 Data
Hypermodel	The modelling features will be developed on the MatLab software platform. According to the general structure of the CHIC project, models will be designed according to an horizontal and a vertical scheme.
Validation Protocol	Validation protocols for the end-users and developers will be continuously updated and the results will be collected in the frames of the tasks bellow. Task 12.3: Training activities (M12-48) SubTask 12.3.a: Workshops/Summer schools In order to train potential users on the use of the CHIC platform and get

	feedback from them from early on in the project's lifetime, a series of workshops/summer schools will be organised starting after the end of the first year until the end of the project with a minimum of three events organised (MS31, MS32, MS33). The validation protocol could be based on the attached Evaluation and Validation Protocol Template, Version 0.1 (Appendix 4).
Usage Survey	Questionnaire for usage of models and hypermodels in the clinical setting (Appendix 3) is elaborated and the data collection has been initiated. The collected results will be reported in the frames of the training events and to CHIC platform developers.

5 Criteria-Based Assessment Check-List

A criteria-based assessment gives a measurement of quality and is derived from ISO/IEC 9126-1 Software engineering - Product quality. This check list is adapted from the Software Evaluation Guide elaborated by Mike Jackson, Steve Crouch and Rob Baxter from The Software Sustainability Institute[5].

Requirement	Sub-requirement	Met by
Usability	Understandability	Easily understood?
	Documentation	Comprehensive, appropriate, well-structured user documentation?
	Buildability	Straightforward to build on a supported system?
	Installability	Straightforward to install on a supported system?
	Learnability	Easy to learn how to use its functions?
Sustainability and maintainability	Identity	Project/software identity is clear and unique?
	Copyright	Easy to see who owns the project/software?
	Licencing	Adoption of appropriate licence?
	Governance	Easy to understand how the project is run and the development of the software managed?
	Community	Evidence of current/future community?
	Accessibility	Evidence of current/future ability to download?
	Testability	Easy to test correctness of source code?
	Portability	Usable on multiple platforms?
	Supportability	Evidence of current/future developer support?
	Analysability	Easy to understand at the source level?
	Changeability	Easy to modify and contribute changes to developers?
	Evolvability	Evidence of current/future development?
	Interoperability	Interoperable with other required/related software?

Appendix 2 presents the extended version of the suggested for implementation criteria-based assessment check-list.

[5] Software Evaluation Guide, By Mike Jackson, Steve Crouch and Rob Baxter from The Software Sustainability Institute, http://software.ac.uk [May 2014]

6 GCP Validation Check-List

Good Clinical Practice (GCP) is an international ethical and scientific quality standard for designing, recording and reporting trials involving human subject participation. GCP standards have been explored and described in detail and the compliance activities have been reported and presented in the frames of p-medicine project.[6] The information bellow has been adapted from the available p-medicine project's public deliverables and more specifically:

- D2.1 State of the art review of the p-medicine environment
- D2.2 Definition on scenarios and use cases and report on Scenario based user needs and requirements
- D5.5 Report on legal and ethical issues for p-medicine tools used for international GCP trials
- D6.1 Report on use cases, scenarios, user needs, tools, interoperability issues for the ECRIN community
- D9.1 Report on regulatory and international aspects of the clinical trials
- D9.3 Report on the validation and certification of ObTiMA and DoctorEye

The basic principles of GCP are:

1. Clinical trials should be conducted in accordance with the ethical principles that have their origin in the Declaration of Helsinki and that are consistent with GCP and the applicable regulatory requirement(s).
2. Before a trial is initiated, foreseeable risks and inconveniences should be weighed against the anticipated benefit for the individual trial subject and society. A trial should be initiated and continued only if the anticipated benefits justify the risks.
3. The rights, safety and well-being of the trial subjects are the most important considerations and should prevail over interests of science and society.
4. The available nonclinical and clinical information on an investigational product should be adequate to support the proposed clinical trial.
5. Clinical trials should be scientifically sound and described in a clear, detailed protocol.
6. A trial should be conducted in compliance with the protocol that has received prior Institutional Review Board (IRB)/Independent Ethics Committee (IEC) approval/favourable opinion.
7. The medical care given to, and medical decisions made on behalf of, subjects should always be the responsibility of a qualified physician or, when appropriate, of a qualified dentist.
8. Each individual involved in conducting a trial should be qualified by education, training, and experience to perform his or her respective task(s).
9. Freely given informed consent should be obtained from every subject prior to clinical trial participation.

[6] p-medicine project, http://p-medicine.eu [May 2014]

10. All clinical trial information should be recorded, handled, and stored in a way that allows its accurate reporting, interpretation and verification.
11. The confidentiality of records that could identify subjects should be protected, respecting the privacy and confidentiality rules in accordance with the applicable regulatory requirement(s).
12. Investigational products should be manufactured, handled, and stored in accordance with applicable Good Manufacturing Practice (GMP). They should be used in accordance with the approved protocol.
13. Systems with procedures that assure the quality of every aspect of the trial should be implemented.

The suggested requirements description for CHIC project clinical trials related activities, tools and models are the "Standard requirements for GCP compliant data management in multinational clinical trials" of the European Clinical Research Infrastructures Network (ECRIN) Working Group on Data Centres Version 1 from 27 May 2010.

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

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

Each individual requirement is categorized as either a minimal (min) requirement or best practice (bp).

6.1 IT Requirements

6.1.1 IT01 - Procurement and Installation (Servers)

IT01 section has 3 minimal and 2 best practice requirements.

Key Requirement	*Met by*
IT01.01 min Server Specification	Servers and similar equipment should be specified and selected according to the specific requirements of the trials unit and the functions being supported
IT01.02 min Server Builds	Detailed records of builds must be available, for maintenance and safe rebuilding
IT01.03 min Warranties and Support	Sufficient support arrangement should be in place for the expected lifetime of the equipment
IT01.04 bp Server Procurement	Purchases should show evidence of appropriate selection between alternative suppliers and / or comply with policies stipulated by the host organisation
IT01.05 bp Procurement Planning	There should be a defined retirement / replacement policy for servers, given expected lifetimes

6.1.2 IT02 - Physical Security and Management

IT02 section has 4 minimal and 6 best practice requirements.
Many of the functions listed below may be outside the direct control of the trials unit, and **formal documents/agreements** should therefore be available to provide evidence that the standards are being met.

Key Requirement	*Met by*
IT02.01 min Locked Server Room	Servers must be housed within a dedicated locked room with unescorted access limited to specified individuals
IT02.02 min Secured Power Supply	The power supply to servers should be secured, e.g. by a UPS unit, to allow an orderly shutdown on power failure
IT02.03 min Encryption of non physically secure data	No patient data should be stored on anything other than protected servers (e.g. on laptops, desktops, USB sticks etc.) unless it is encrypted
IT02.04 min Server Failure - Response	Alerts on server failure within normal business hours should be sent automatically to relevant personnel
IT02.05 bp Server Failure - Response 24/7	Alerts on server failure outside of normal business hours should be sent automatically to relevant personnel
IT02.06 bp Controlled Environment	Servers should be housed in a temperature controlled environment
IT02.07 bp Theft and Malicious Damage	The server room/building should have an alarm system with the alarm linked to a central response centre
IT02.08 bp Hazard Control - Fire Alarms	The server room should be fitted with heat and smoke alarms, monitored 24/7
IT02.09 bp Hazard Control - Fire Response	The server room should be fitted with automatic fire response measures (e.g. inert gas)
IT02.10 bp Hazard Control - Water	Water ingress (e.g. from external flooding)

6.1.3 IT03 - Logical Security and Management

IT03 section has 7 minimal and 4 best practice requirements.
Again there may be a need for **formal documents/agreements** between the data centre and the organisation (e.g. the host university, a hosting service) that may provide or manage many of these facilities.

Key Requirement	*Met by*
IT03.01 min Security	Regular reviews of IT security systems, practices and documentation, followed by any necessary planning and

Management System	actions, should occur as part of an ongoing Security Management System
IT03.02 min Commitment to Data Protection	The unit or its parent organisation can demonstrate compliance with and commitment to local data protection legislation, including relevant policies, training and individuals with designated roles (e.g. 'Data protection officer')
IT03.03 min External Firewalls	External firewalls should be in place and configured to block inappropriate access
IT03.04 min Encrypted Transmission	Clinical data transmitted over the internet to or from the trials unit must be encrypted
IT03.05 min Server Admin Role	Servers should be protected by a highly restricted administrator password (i.e. known to essential systems staff only)
IT03.06 min Admin Password Management	The administrator password should be changed regularly according to locally agreed policies, and stored securely for emergency use (e.g. off site)
IT03.07 min Server Maintenance	Necessary patches and updates should be identified and applied in a timely but safe manner to: ... • the operating system, • anti-malware systems, • backup systems and • major apps (e.g. Clinical DBMSs, Web servers, Remote Access systems, • etc.)
IT03.08 bp Commitment to Information Security	The unit or its parent organisation can demonstrate management commitment to information security, including relevant groups, policies, training and individuals with designated roles (e.g. 'IT security officer')
IT03.09 bp Internal Firewalls	Internal firewalls should be in place and correctly configured, e.g. blocking access to other departments, students
IT03.10 bp Security Testing	Regular security testing should be carried out and is documented
IT03.11 bp Traffic Monitoring	Traffic activity should be monitored and hacking attempts identified and investigated

6.1.4 IT04 - Logical Access Control

IT04 section has 7 minimal and 1 best practice requirements.

Key Requirement	*Met by*
IT04.01 min Logical Access Procedures	Standard Operating Procedures (SOPs) and policies for access control to the network(s) and specific systems should be in place
IT04.02 min Access Control	Each system requiring access controls should have mechanisms, e.g. using roles, group membership, etc., that

Management	can be used to effectively differentiate and manage access
IT04.03 min Granularity of Access	Access control mechanisms should be granular enough so that users only see the data they need to see
IT04.04 min Password management	Network password management should be enforced on all users, including regular password change and password complexity
IT04.05 min Remote Access	Remote access (e.g. via Citrix) should be controlled to the same standards as above, and should not normally include access to the host's network
IT04.06 min Desktop Lockout	Desktop logins should post a blank screen or screensaver after a locally determined shut down period, and require password re-activation
IT04.07 min Control - Clinical Data	Access rights to Clinical Data Systems should be regularly reviewed, changes to access requested and actioned according to defined procedures, by designated individuals, with records kept of all rights, when granted, why and by whom.
IT04.08 bp Control - General	Access rights to the network and general should be regularly reviewed, changes to access requested and actioned according to defined procedures, by designated individuals, with records kept of all rights, when granted , why and by whom

6.1.5 IT05 - Business Continuity

IT05 section has 6 minimal and 7 best practice requirements.

Key Requirement	*Met by*
IT05.01 min Business Continuity Plan	A Business Continuity plan should be present, covering likely action in the event of a major loss of function (e.g. fire, long term power failure, full server failure, sudden loss of key staff)
IT05.02 min Back Up Policies	Documents detailing backup policy, procedures, restores and testing must be in place
IT05.03 min Back Up Frequency	Back ups must be taken at least once every 24 hours, using a managed, documented regime
IT05.04 min Back Up Storage	Back up media should be stored in a fire proof safe
IT05.05 min Recovery Testing	Testing of full restore procedures, back to the original server, should take place at least annually
IT05.06 min Off site archiving	The back up regime should involve regular offsite storage of archive media (e.g. monthly)
IT05.07 bp Business Continuity Integration	The unit's Business Continuity (BC) should be integrated with the host organisation's BC plan and appropriate access arranged
IT05.08 bp Specified Downtime	A trials unit should state, and adhere to, a specific maximum downtime to any potential user

IT05.09 bp Business Continuity Review	Regular review, should occur, at least annually, of the detailed BC plan
IT05.10 bp Back up - Transaction Logs	Transaction log backups should take place regularly through the working day, according to a locally agreed plan
IT05.11 bp Back up - Environment	The server / DBA environment (groups, log-ins, jobs etc.) should be captured and restorable
IT05.12 bp Back up - Warm / Hot Failover	Log shipping or a mirroring procedure should be in place to a warm / hot failover system
IT05.13 bp Failover testing Recovery	If available, testing of full restore procedures from a warm / hot failover system should take place at least annually

6.1.6 IT06 - General System Validation

IT06 section has 9 minimal and 0 best practice requirements.
In practice, different systems have very different validation requirements, we need to be able to justify the decisions taken and the implemented validation plans/guides (e.g. GAMP® - Guide for Validation of Automated Systems).

Key Requirement	*Met by*
IT06.01 min Validation Policies	Policies and SOPs should be in place covering system validation systems and processes
IT06.02 min Validation master plan	The unit should have a validation master plan in place, identifying systems, the risks associated with each, and the consequent validation strategy for each
IT06.03 min Risk based approach	The general approach to validation of any system should be based on analysis of potential risk, and take into account the system's usage, users and origins
IT06.04 min Individual validation plans	Detailed validation plans should exist for any particular system, in line with the master plan and policies described above, detailing the validation required, how and when it should be done, and how it should be recorded
IT06.05 min Summaries and Recording	A signed and dated summary of the results of each major validation episode should exist, for each system being validated
IT06.06 min Detailed Evidence	More detailed evidence - e.g. of test results or signed user statements - should be available as evidence for the summary validation documents
IT06.07 min Change Control Policies	Policies and SOPs should be in place defining change control mechanisms and their scope, who should authorise and review requests, and how they should be documented
IT06.08 min Change and Re-	Changes in systems should result in a review of the need for revalidation

validation	
IT06.09 min Software Development	Evidence should be available that Quality Assurance (QA) processes during software development have been implemented properly

6.1.7 IT07 - Local Software Development

IT07 section has 1 minimal and 4 best practice requirements.

Key Requirement	*Met by*
IT07.01 min Documentation of in-house software	All modules should be fully documented and specify inputs, outputs, purpose as well as a description of internal mechanisms and algorithms
IT07.02 bp Code Review	Regular review and walk through of program code should occur
IT07.03 bp Re-usable Modules	A library of reusable validated code/modules/components should be developed
IT07.04 bp Development Model	*A V-model based procedure is recommended, with constituent modules first validated individually and then integrated before re-validation at the system level*
IT07.05 bp In line Commenting	All code should have sufficient in line documentation to support tracing of program execution

6.1.8 IT08 - Clinical DBMS Systems

IT08 section has 2 minimal and 6 best practice requirements.

Key Requirement	*Met by*
IT08.01 min Development and Production Instances	The system offers two instances: development and production
IT08.02 min Timestamp Control	Time synchronization within the Clinical Data Management System (CDMS) is ensured. Sites using electronic Remote Data Capture (eRDC) are not able to change the system's time stamp
IT08.03 bp Metadata Audit Trail	An audit trail for metadata changes is implemented
IT08.04 bp Available audit trail	The audit trail for any particular data item is visible
IT08.05 bp Searchable audit trail	The audit trail is searchable and capable of producing audit trail reports
IT08.06 bp Development, Production and Test Instances	The system offers three instances: development, test, production. The test environment and the production environment are identical
IT08.07 bp	Systems support a full range of accented Latin characters

Latin Characters	
IT08.08 bp Date/numerical Representation	It is possible to set and use different date and numerical representations in the system

6.1.9 IT09 - Treatment Allocation Systems

IT09 section has 3 minimal and 1 best practice requirements.

Key Requirement	*Met by*
IT09.01 min Documentation & Validation	The underlying logic and operations of all systems for allocating subjects to treatments must be clearly documented and validated
IT09.02 min Record of Allocation	A record of all allocation material generated (e.g. randomisation lists) and all decisions made (e.g. within a dynamic balancing system) must be maintained
IT09.03 min Failover to Manual	System(s) must be in place, supported by training, to deal with a loss of normal electronic randomisation
IT09.04 bp Monitoring	The randomness of list generation or minimisation should be monitored in the context of any particular trial

6.1.10 IT10 - Reporting

IT10 section has 3 minimal and 10 best practice requirements.

Key Requirement	*Met by*
IT10.01 min Report access control	Access to different reports should be controlled and match the users' requirements
IT10.02 min Report Validation	The structure and accuracy of reports should be validated against the source data, frequency of validation being determined by a change control process
IT10.03 min Single Subject Data	It should be possible to examine and export a full record of a single subject's data (excluding personal identifying data)
IT10.04 bp Standard Reports	A set of frequently required (parameterised) reports should be available to appropriate users
IT10.05 bp UI Ad Hoc Reports	It should be possible to extract ad-hoc filtered datasets (reports) via the UI
IT10.06 bp Audit Data	Selected reports should include the option of including audit related data
IT10.07 bp Report Rerun	Once a report is parameterised by user it should be possible to save and rerun it
IT10.08 bp Metadata included	The option should exist to include a metadata description of extracted data
IT10.09 bp	Standard reports should include the details of the current study definition in

Study definition	an approved XML schema (trial schedule and data items)
IT10.10 bp Format of Reports	Report data can be generated / exported in formats agreed with local report consumers , e.g. PDF, HTML, XML
IT10.11 bp Data Personnel	It should be possible to examine and export a record of a single data entry clerk's input data
IT10.12 bp Key Field Changes	It should be possible to examine and export a full list of changes to identified key fields, e.g. fields reporting toxicity as part of monitoring
IT10.13 bp Automatic Generation	The generation of reports can be automated and can be scheduled

6.1.11 IT11 - Data Export

IT11 section has 6 minimal and 2 best practice requirements.

Key Requirement	*Met by*
IT11.01 min Data Export Procedures	SOPs and policies for data exports should be in place
IT11.02 min Encryption of PID	The inclusion of any patient identifiable data means any exported file(s) must be encrypted
IT11.03 min Purpose Recorded	The purpose of the planned data transfer(s) and the nature of any further processing / transfer planned for the data should be known and logged
IT11.04 min Assuring Security	The unit sending the data must have a written agreement/declaration from the recipient that the receiving organization will maintain appropriate security of data
IT11.05 min Records of Transfers	Details of any specific data transfer should be logged, including list of data items, sender, recipient and transfer method, and the date sent
IT11.06 min Retention of Copies	Copies of the data sent should be retained within a read only regime and be available as a reference data set for audit/reconstruction purposes
IT11.07 bp Format of Transfers	The format of data should be as specified by the recipient
IT11.08 bp Electronic Archiving	Standardised formats for electronic archiving (e.g. ASCII, PDF, XML, CDISC ODM, FDA approved SAS format) are used

6.1.12 IT12 - Importing & Uploading Data

IT12 section has 3 minimal and 2 best practice requirements.

Key Requirement	*Met by*
IT12.01 min Upload Procedures	SOPs and policies for importing / uploading data should be in place

IT12.02 min File Retention I	The original files received should be retained within a read only regime, and be available as a reference data set for audit/reconstruction purposes
IT12.03 min Logging of Uploads	Each upload process should be documented and logged
IT12.04 bp File Retention II	Any files prepared from the originals and used as the direct source of the upload should be kept securely within a read only regime for audit/reconstruction purposes
IT12.05 bp Data Validation on Input	Data uploaded to clinical data systems should be checked and annotated as per normal data entry

6.1.13 IT13 - Directly Amending Data

IT13 section has 2 minimal and 0 best practice requirements.

Key Requirement	*Met by*
IT13.01 min Requests for Amendment	Any requests must be in writing and retained, and must include the justification for the change
IT13.02 min Recording Amendments	Any changes made must be logged and the details noted

6.1.14 IT14 - Delivery of Data for Analysis

IT14 section has 3 minimal and 1 best practice requirements.

Key Requirement	*Met by*
IT14.01 min Preparation for Analysis Procedures	SOPs and policies for generating and preserving datasets for analysis should be in place
IT14.02 min R/O Analysis Data Retention	The base data provided for analysis is retained within a read only regime, and is available as a reference data set for any future re-analysis or audit
IT14.03 min Extracted Data Validation	The data generated for analysis, and / or the extraction process, should be validated against the source data in the clinical database (not necessarily by IT staff)
IT14.05 bp Extracted Data - Formats	The data generated can be generated in Stata, SAS, R and SPSS native formats (as well as CSV, XML)

6.1.15 IT15 - Long Term (electronic) Data Curation

IT15 section has 4 minimal and 5 best practice requirements.

Key Requirement	*Met by*
IT15.01 min Data Preparation Policies	Policies / SOPs about what data would normally be curated (should normally include metadata, the protocol and other documents as well as all clinical data) should be in place

IT15.02 min Data Retrieval from Curation	Policies / SOPs about how data would normally be retrieved/ accessed, and who is authorised to do so by the sponsor / investigator, should be in place
IT15.03 min Data Destruction	Final destruction of data, if required /allowed, should be as specified by regulations, funding body and/or sponsor
IT15.04 min Recovery Testing	The recovery process(es) should be documented and tested
IT15.05 bp Data Preparation formats	Data from databases should be decrypted if necessary and transformed into pre-approved XML schemas (e.g. CDISC ODM, Data Documentation Initiative (DDI) 3), or into plain ASCII text files
IT15.06 bp Data Preparation - Identifiers	Subject identifiers should be reduced to a minimum or removed altogether, depending on policies / requirements
IT15.07 bp Data Preparation - Records	The data preparation process, its inputs, dates and details, should be logged
IT15.08 bp Additional Material Generation	Additional electronically stored material may be generated to ensure copies of paper only documents are available (i.e. by scanning)
IT15.09 bp Curation Facilities	Service level agreements should be in place with specialist curation providers, providing physical and logically secure long term storage

6.2 Data Management Requirements

6.2.1 DM01 - Clinical Data Management Application - Design and Development

DM01 section has 10 minimal and 6 best practice requirements.

Key Requirement	*Met by*
DM01.01 min Development Lifecycle Policy	SOPs covering the development lifecycle of the clinical data management application and the CRF (incl. development, testing and deployment) should be in place
DM01.02 min Design of CRFs	Process of CRF design is documented, reviewed and includes version management
DM01.03 min Cross-disciplinary Team	Clinical data management application and CRF development is performed by a cross- disciplinary team (e.g. programmer, trial manager, statistician, data manager)
DM01.04 min Requirement	The requirements specification for the CRF is driven by the protocol (e.g. primary safety and efficacy

Specifications of CRF	variables) and takes into consideration the workflow of trial procedures and organizational aspects
DM01.05 min Standardized Questionnaires /Instruments	Validated questions, scales or standard instruments are used where possible (e.g. quality of life questionnaires) and the integrity of validated questionnaires is maintained
DM01.06 min Data Non-redundancy	CRF does not duplicate data (e.g. no redundant questions, if not for validation / data management purposes) or calculates results unnecessarily
DM01.07 min Functional Specifications of CRFs	CRF functional specifications exist identifying each data item on each CRF (including field names, types, units, validation logic, conditional branching)
DM01.08 min Checking of clinical data management application	Procedures are implemented for checking (e.g. proofreading) the clinical data management application including eCRF and pCRFs against specifications and protocol
DM01.09 min Delivery of CRFs	CRFs are delivered to sites prior to enrolment
DM01.10 min Evaluation of CRF Usability	The usability of eCRFs is evaluated and assessed before deployment to live environment
DM01.11 bp Review of CRFs	CRFs are reviewed against the protocol, end-user expectations and CRF design best practice (e.g. use of validated questionnaires). An acceptance test for CRFs is conducted
DM01.12 bp Use of Interim CRF	In cases of eCRF an interim CRF (iCRF) should be available to allow data to be accurately recorded / collated at sites prior to data entry for emergency cases (e.g. if eCRF not available)
DM01.13 bp Documentation Principles	Common documentation principles are applied to data items (e.g. preferred coding system, numbering of items, types of missing data, complete answer categories, preference for positive formulated questions, etc.)
DM01.14 bp Libraries and Metadata Repositories	Libraries with procedures concerning library management and/or a metadata repository are used, enabling reuse of predefined data items/forms
DM01.15 bp Quality Management	Quality documents covering good design practice, usability, local design conventions, etc. are available
DM01.16 bp User Friendliness of CRFs	CRFs are divided into appropriate sections with simple and clear instructions for completion and use consistent design principles

6.2.2 DM02 - Clinical Data Management Application - Validation

DM02 section has 7 minimal and 2 best practice requirements.

Key Requirement	*Met by*

DM02.01 min Clinical Data Management Application Policies	SOPs and policies for clinical data management application and CDMS validation are in place
DM02.02 min Trial-specific Test Plan	A trial-specific test plan defines the test methodology, covering scope of test, item pass/fail criteria, etc.
DM02.03 min Test against Functional Specifications	The testing with sample data against functional specifications is carried out before deployment to live environment
DM02.04 min Test of Data Checks	Tests of all validation checks and conditional data capture mechanisms, plus any derivations are conducted, documented and retained
DM02.05 min Validation Report	Data validation final report for the trial has to be provided and signed by responsible DM person
DM02.06 min CRF Approval	Approval of the CRF is signed off by key persons
DM02.07 min Check of Validation Programs, Lists and Scripts	Validation programs, lists and scripts are checked, tested, documented and retained
DM02.08 bp Validation against Specifications	The process of clinical data management application design and data checks programming is validated against specifications
DM02.09 bp Validation Report Generation	System is able to generate reports used for validation

6.2.3 DM03 - Clinical Data Management Application - Change management

DM03 section has 6 minimal and 3 best practice requirements.

Key Requirement	*Met by*
DM03.01 min Change Management of Clinical Data Management Application	SOPs and policies for clinical data management application change management are in place, including last minute chances
DM03.02 min Change Management of Metadata	Individual requests for change to metadata (e.g. meta-data, specification of CRF) are justified, itemized and recorded by authorised personnel
DM03.03 min	A risk analysis is conducted before major amendment for change. For each

Amendment for Change	major change the changes, implications and consequent further actions are recorded
DM03.04 min Test of Amendments	Any amendment is tested in the test environment, following test specifications and the test results are recorded
DM03.05 min Renewed Training	In the case of significant changes, the need for retraining is evaluated and implemented if necessary
DM03.06 min Information of Changes	Mechanisms are implemented to easily inform relevant staff and users of changes, and provide support and explanatory material as required
DM03.07 bp Requirements for amended CRF	An amended CRF (that may require ethical approval) has to conform to requested amendments and/or revised protocol. Trial amendments, that may have consequences on the CRF, are taken into consideration
DM03.08 bp CRF-versioning	CRF page numbering and version information is always updated to reflect the current status
DM03.09 bp Management of Change Requests	Change requests are accumulated to minimize amendments

6.2.4 DM04 - Treatment Allocation and (Un)Blinding Management

DM04 section has 8 minimal and 0 best practice requirements.

Key Requirement	*Met by*
DM04.01 min Policies for the Implementation of Randomisation	SOPs and policies for the set up of randomisation in any particular trial are in place
DM04.02 min Policies for ensuring Randomisation /Blinding	SOPs and policies exist for protection of blinding and conservation of random allocation to treatment groups
DM04.03 min Policies for Unblinding	SOPs are in place to support rapid and safe unblinding of blinded treatments
DM04.04 min Specification of Randomisation	Specification for the underlying system(s) or the specific trial randomisation process is available
DM04.05 min Randomisation Implementation	The randomisation implementation for any particular trial conforms to the protocol
DM04.06 min Specification of the Randomisation Design	The study statistician is responsible for the specification of the randomisation design. A randomisation specification document is provided

DM04.07 min Problem Management of Randomisation	Any problems that arise in the randomisation process are logged and the subsequent actions recorded
DM04.08 min Randomisation Training	All staff who handles randomisation requests is adequately trained for each specific trial randomisation process

6.2.5 DM05 - Site Management, Training & Support

DM05 section has 6 minimal and 0 best practice requirements.

Key Requirement	*Met by*
DM05.01 min Policies for Site Opening	SOPs or policies for opening a centre for data collection are in place
DM05.02 min User Training for Data Entry	User training with data entry instructions or guidelines, for both pCRFs and eCRFs, is provided for relevant site staff and is documented
DM05.03 min Test or Productive Environment	It is clearly indicated to the user whether they are working on a test eCRF or whether the "real trial" has been opened
DM05.04 min Access to Production System	Site has access to production data systems only once all relevant paperwork and training has been completed; including ethical and research approvals, contracts, site initiation
DM05.05 min Site Documentation	After significant changes site documentation is updated
DM05.06 min Responsibility list	An up to date list of who can do what at each site, including complete CRFs, i.e. a ‘delegate log’, is maintained

6.2.6 DM06 - Data Entry and Processing

DM06 section has 12 minimal and 3 best practice requirements.

Key Requirement	*Met by*
DM06.01 min Data Entry Policies	SOPs and policies for data entry and corrections are in place
DM06.02 min Restriction of Data Access	Site staff have access only to data of their site
DM06.03 min Data Security	Data manager and IT-staff involved will keep data secure and confidential at all times
DM06.04 min System Security	System security and access control is ensured, data is only accessible to authorised personnel
DM06.05 min	A CRF tracking system is in place

Tracking of CRFs	
DM06.06 min Management of missing CRFs	Systems identify and report on missing or late CRFs /data
DM06.07 min Quality of Received Data	Data received is checked (pCRF and eCRF)
DM06.08 min Data Confidentiality	The blinding of information submitted to the data centre with regard to subject identifying information conforms to national requirements (pseudonymisation)
DM06.09 min Self Evident Corrections	Clear guidelines and procedures exist to carry out self evident corrections
DM06.10 min Simple Checks	Simple checks (e.g. range checks) should be available with the possibility to unset for pCRF entry
DM06.11 min Complex Checks	Complex checks with critical variables (e.g. crossform validation) are available
DM06.12 min Audit Trail	All transactions to the trial database (insert, update, delete) have a clear and complete audit trail, covering the date and time of the input, the person making the change and the old and new values
DM06.13 bp Timelines for Data Entry	Time-lines for data entry are considered
DM06.14 bp Amendment / Truncation of Schedules	Logging systems can easily truncate and / or amend schedules to maintain accuracy in identifying outstanding data
DM06.15 bp Data Deletion	Complete deletion of data from the system is prevented unless it is to comply with a legal request. If indicated for legal reasons, total deletion only takes place using specified procedures and recording with explanatory information

6.2.7 DM07 - Data Quality Checks

DM07 section has 6 minimal and 2 best practice requirements.

Key Requirement	*Met by*
DM07.01 min Data Quality Policies	SOPs and policies are in place regarding data checking, and refer as necessary to the protocol, agreed instructions, GCP and regulatory requirements
DM07.02 min Batch Validation Checks	Validation checks are able to be executed via a batch process, to identify new warnings, missing, illogical and inconsistent data
DM07.03 min Data Review	Systems are able to support data checks by generating specified data in formats that match input format (e.g. that mimic CRFs) for manual review of data, e.g. medical consistency checks, lab data pointing to an AE
DM07.04 min Risk Based	A risk based source data verification regime is implemented as specified in the protocol, with the emphasis on primary target variables and other

Source Data Verification	essential data. A check of primary endpoints and other essential data is conducted
DM07.05 min Documentation of Checks	All data checking exercises are documented
DM07.06 min Problem Management	Problems and issues are reported to the appropriate person for query generation or other resolution
DM07.07 bp Quality Monitoring of Sites	Centres are monitored for quantity / types of errors to identify potential problems, e.g. with particular preset trigger levels
DM07.08 bp Statistical Evaluation of Data Quality	Statistical methods are used to assess and evaluate data quality (e.g. easures to analyse possible problems and irregularities should cover e.g. multivariate analysis of possible outlier candidates, conspicuous data patterns, preferred numerical sequences, accumulation of values close to defined limits) and the impact on analysis should be evaluated

6.2.8 DM08 - Query Management

DM08 section has 5 minimal and 4 best practice requirements.

Key Requirement	*Met by*
DM08.01 min Query Policies	SOPs and policies are available covering query format, generation, timelines, data change and resolution
DM08.02 min Query Resolution	Procedure for resolving of queries exist
DM08.03 min Query Creation and Tracking	Queries are created in accordance with specifications and documented procedures
DM08.04 min Responses to Queries	Responses are recorded when returned, identified when outstanding and resent as necessary
DM08.05 min Actions in Response to Queries	Query resolution tracked and appropriate action taken within agreed timelines and documented in the audit trail
DM08.06 bp Issuing of Queries	Queries are issued to sites within agreed timelines
DM08.07 bp Avoidance of Query Duplications	Systems avoids accidental duplication of queries
DM08.08 bp Generation of Messages	System is able to generate messages to users not linked to specific data items (i.e. information giving, not expecting a reply)
DM08.09 bp Generation of Query Reports	Reports are generated showing query generation data, return times etc. broken down by site, by source form, etc.

6.2.9 DM09 - Data Coding and Standards

DM09 section has 4 minimal and 4 best practice requirements.

Key Requirement	*Met by*
DM09.01 min Policies for Coding	SOPs and policies for coding are in place (e.g. to promote consistency and proper use of versions)
DM09.02 min Coding Training	Coding or categorisation is carried out by personnel trained on the relevant systems
DM09.03 min Support of CONSORT[7]	The protocol, clinical data management application and CRF, should support the CONSORT trial reporting requirements
DM09.04 min Coding of SAEs	The constituent symptoms of all Serious AEs are coded prior to analysis (e.g. MedDRA for drugs)
DM09.05 bp Use of Standards for Coding	Coding uses named standard systems for particular types of data (e.g. MedDRA) where possible
DM09.06 bp Consistency of Coding	Coding uses consistent systems across different trials and follow consistent conventions and rules in their use
DM09.07 bp Coding of AEs	The constituent symptoms of all AEs should be coded prior to analysis
DM09.08 bp Autocoding	Use of autoencoder(s) and synonym list(s) where possible, however within well defined limits and with authorisation from senior staff, otherwise manual coding is performed

6.2.10 DM10 - Safety Data Management Application

DM10 section has 4 minimal and 2 best practice requirements.

Key Requirement	*Met by*
DM10.01 min Policies for Safety Data Management	SOPs and policies for safety data management are in place
DM10.02 min Safety Data Management	Safety data management application allow the logging of all forms, faxes and correspondence involved, and subsequent information / evaluation requests
DM10.03 min Expedited Reporting	Safety data management application supports expedited reporting to authorities
DM10.04 min Routine Reporting	Safety data management application supports routine reporting to all relevant authorities when required (e.g. annual line listings)
DM10.05 bp Electronic Reporting	Safety data management application supports reporting via electronic transfer to authorities

[7] http://www.consort-statement.org

DM10.06 bp Safety Data Reconciliation	Safety data management application supports the reconciliation of SAEs with other safety data

6.2.11 DM11 - Pre-Analysis Data Management

DM11 section has 5 minimal and 2 best practice requirements.

Key Requirement	*Met by*
DM11.01 min Policies for Data Base Locking	SOPs and policies regarding taking a fixed image of the database (snapshot) and, if required,, 'locking' and 'unlocking' databases are in place. In case a locked database is unlocked a documented reason is provided
DM11.02 min Data Completion	All relevant data (or all except for a pre-defined / preagreed fraction) have been received prior to data extraction for analysis (database lock)
DM11.03 min Query resolution completion	All queries (or all except for a pre-defined / pre-agreed fraction) have been resolved
DM11.04 min Data Reconciliation	All external data (e.g. safety database, lab data) has been reconciled
DM11.05 min Data Base Consistency Check	Relevant batch consistency checks of database have been completed and actioned
DM11.06 bp Review of Coding	All relevant coding has been reviewed
DM11.07 bp Data Base Audit	Database audit should be carried out, documenting error rate

6.2.12 DM12 - Managing (physical) Archives

DM12 section has 5 minimal and 0 best practice requirements.

Key Requirement	*Met by*
DM12.01 min Policies for Archiving	SOPs and policies are in place concerning physical archiving of essential trial documents
DM12.02 min Access to Archive	Access to study archive is documented
DM12.03 min Protection of Archive	Measures are in place to guarantee safe archiving (e.g. locked rooms and fire-proof cupboards, safe area, protected and controlled access for authorized staff only)
DM12.04 min Archiving Duration	Essential trial documents (including data) are archived for as long as specified by protocol, regulations, funding body and/or sponsor
DM12.05 min	Conduct of trial can be reconstituted from archived essential trial

Trial Reconstitution	documents

6.3 International Aspects Requirements

6.3.1 IN01 - International Aspects

IN01 section has 1 minimal and 3 best practice requirements.

Key Requirement	Met by
IN01.01 min User Support	eRDC Help Desk and Hot Line is provided covering user hours
IN01.02 bp CRF Translation	If necessary, CRFs/eCRFs can be translated into the language(s) required for the trial, including messages associated with error checking. Translations are verified
IN01.03 bp Support of National Regulations	Application display, change or hide questions / CRFs to better support national legislation (without using different versions)
IN01.04 bp Multilingual User Support	Help desk and hot line can deal with the language of the users and provide some sort of help

6.4 Trials Unit Staff Competence Requirements

6.4.1 SC01 - Trials Unit staff competence

SC01 section has 4 minimal and 2 best practice requirements.

Key Requirement	Met by
SC01.01 min Policies for Training	SOPs and policies are in place describing induction and training requirements / policies / procedures
SC01.02 min Staff Competence	DM-staff is competent, trained or being trained to do the job(s) required of them
SC01.03 min Documentation of Training	Records of training are kept for all DM-staff, kept centrally and / or by the staff themselves
SC01.04 min Staff Support	Help and support for DM-staff is available
SC01.05 bp Planning of Staff Training	Training plans are linked to annual appraisal
SC01.06 bp Ticketing System	A formal mechanism for requesting support and logging requests / actions should exist

7 Conclusion

This report presents in concrete details, tailored as innovative check-lists, the advanced set of guidelines, evaluation and validation requirements to support all project partners as well as the external evaluators to standardize the clinical adaptation and validation process of CHIC platform tools, functionalities and frames with special focus on clinical and translational scenarios.

Considering the scenario based user needs and requirements this document defines evaluation and validation criteria and identifies specific objectives (requirements) to be followed during the continuous validation process.

Procedures in monitoring the development of hypermodels according to the defined evaluation and validation criteria are elaborated and criteria for their execution by specific user groups are presented. The work and related activities from other EU research projects have been considered and mentioned.

In general terms the developmental process started from the description of the scenarios to answer the clinical relevant questions. It ends with the validation of the hypermodels with prospective data. Nevertheless, we managed to elaborate an extended evaluation and validation approach, enriched with the inclusion of the validation protocol template (Appendix 4) based on the check-lists bellow:

- General Validation Check-List
- Criteria-Based Assessment Check-List
- GCP Validation Check-List

From the perspective of evaluation and validation of clinical scenarios described in the frames of CHIC project document D 2.2 - “Scenario based user needs and requirements”, one general (with end user interfaces and functionalities) and four specific validation check-lists have ben elaborated and proposed for usage:

- Scenarios for Nephroblastoma Check-List
- Scenarios for Glioblastoma Check-List
- Scenarios for Non-Small-Cell Lung Cancer (NSCLC) Check-List
- Scenarios for prostate cancer Check-List

Regardless of the apparent complexity, this approach will simplify and will align to the top software development standards the CHIC platform development process with its related tumor models and hypermodels and will be in line with GCP requirements. All project partners are encouraged to consult this document in order to align their activities to the presented validation check-lists.

Despite the early stage of project implementation we have elaborated the “Questionnaire for usage of models and hypermodels in the clinical setting” (Appendix 3) and the data collection has been initiated. The collected results will be reported to all project partners and in the frames of the next training events and the related deliverables.

8 References

[1] CHIC project, D 2.2 - Scenario based user needs and requirements

[2] P-medicine project deliverables:

- D 2.1 State of the art review of the p-medicine environment
- D 2.2 Definition on scenarios and use cases and report on Scenario based user needs and requirements
- D 5.5 Report on legal and ethical issues for p-medicine tools used for international GCP trials
- D 6.1 Report on use cases, scenarios, user needs, tools, interoperability issues for the ECRIN community
- D 9.1 Report on regulatory and international aspects of the clinical trials
- D 9.3 Report on the validation and certification of ObTiMA and DoctorEye

Appendix 1 – Abbreviations and acronyms

SOA	Service Oriented Architecture
FDA	Food and Drug Administration (US agency)
GMP	Good Manufacturing Practice
ECRIN	European Clinical Research Infrastructures Network
ObTiMA	Ontology-based Trial Management Application
SOP	Standard Operating Procedure
CRF	Case Report Form

Appendix 2 - Detailed software evaluation reports

Usability

Understandability How straightforward is it to understand: • What the software does and its purpose? • The intended market and users of the software? • The software's basic functions? • The software's advanced functions?	**Yes/No, supporting comments if warranted**
High-level description of what/who the software is for is available.	
High-level description of what the software does is available.	
High-level description of how the software works is available.	
Design rationale is available – why it does it the way it does.	
Architectural overview, with diagrams, is available.	
Descriptions of intended use cases are available.	
Case studies of use are available.	

Documentation Looking at the user documentation, what is its • Quality? • Completeness? • Accuracy? • Appropriateness? • Clarity?	**Yes/No, supporting comments if warranted**
Provides a high-level overview of the software.	
Partitioned into sections for users, user-developers and developers (depending on the software).	
States assumed background and expertise of the reader, for each class of user.	
Lists resources for further information.	

Further information is suitable for the level of the reader, for each class of user.	
Is task-oriented.	
Consists of clear, step-by-step instructions.	
Gives examples of what the user can see at each step e.g. screen shots or command-line excerpts.	
For problems and error messages, the symptoms and step-by-step solutions are provided.	
Does not use terms like “intuitive”, “user friendly”, “easy to use”, “simple” or “obviously”, unless as part of quotes from satisfied users	
States command names and syntax, says what menus to use, lists parameters and error messages exactly as they appear or should be typed.	
Uses `teletype-style fonts` for command-line inputs and outputs, source code fragments, function names, class names etc.	
For Java, the package names of classes are stated the first time a class is mentioned.	
English language descriptions of commands or errors are provided but only to complement the above.	
Plain-text files (e.g. READMEs) use indentation and underlining (e.g. === and ---) to structure the text.	
Plain-text files (e.g. READMEs) do not use TAB characters to indent the text.	
API documentation e.g. JavaDoc or Doxygen, documents APIs completely e.g. configuration files, property names etc.	
Is held under version control alongside the code.	
Is on the project web site.	
Documentation on the project web site makes it clear what version of the software the documentation applies to.	

Buildability How straightforward is it to: • Meet the pre-requisites for building the software on a build platform? • Build the software on a build platform?	**Yes/No, supporting comments if warranted**
Web site has instructions for building the software.	
Source distributions have instructions for building the software.	
An automated build (e.g. Make, ANT, custom solution) is used to build the software.	
Web site lists all third-party dependencies that are not bundled, along with web addresses, suitable versions, licences and whether these are mandatory or optional.	
Source distributions list all third-party dependencies that are not bundled, along with web addresses, suitable versions, licences and whether these are mandatory or optional.	
Dependency management is used to automatically download dependencies (e.g. ANT, Ivy, Maven or custom solution).	
All mandatory third-party dependencies are currently available.	
All optional third-party dependencies are currently available.	
Tests are provided to verify the build has succeeded.	

Installability How straightforward is it to: • Meet the pre-requisites for the software on a target platform? • Install the software onto a target platform? • Configure the software following installation for use? • Verify the installation for use? Note that in some cases build and install may be	**Yes/No, supporting comments if warranted**

one and the same.	
Web site has instructions for installing the software.	
Binary distributions have instructions for installing the software.	
Web site lists all third-party dependencies that are not bundled, along with web addresses, suitable versions, licences and whether these are mandatory or optional.	
Binary distributions list all third-party dependencies that are not bundled, along with web addresses, suitable versions, licences and whether these are mandatory or optional.	
Dependency management is used to automatically download dependencies (e.g. ANT, Ivy, Maven or custom solution).	
All mandatory third-party dependencies are currently available.	
All optional third-party dependencies are currently available.	
Tests are provided to verify the install has succeeded.	
When an archive (e.g. TAR.GZ or ZIP) is unpacked, it creates a single directory with the files within. It does not spread its contents all over the current directory.	
When software is installed, its contents are organised into sub-directories (e.g. docs for documentation, libs for dependent libraries) as appropriate.	
All source and binary distributions contain a README.TXT with project name, web site, how/where to get help, version, date, licence and copyright (or where to find this information), location of entry point into user doc.	
All GUIs contain a Help menu with commands to see the project name, web site, how/where to get help, version, date, licence and copyright (or where to find this information), location of entry	

point into user doc.	
All other content distributed as an archive contains a README.TXT with project name, web site, nature, how /where to get help, date.	
Installers allow user to select where to install software.	
Uninstallers uninstall every file or warns user of any files that were not removed and where these are.	

Learnability How straightforward is it to learn how to achieve: • Basic functional tasks? • Advanced functional tasks?	**Yes/No, supporting comments if warranted**
A getting started guide is provided outlining a basic example of using the software.	
Instructions are provided for many basic use cases.	
Instructions are provided supporting all use cases.	
Reference guides are provided for all command-line, GUI and configuration options.	
API documentation is provided for user-developers and developers.	

Sustainability and maintainability

Identity To what extent is the identity of the project/software clear and unique both within its application domain and generally?	**Yes/No, supporting comments if warranted**
Project/software has its own domain name.	
Project/software has a logo.	
Project/software has a distinct name within its application area. A search by Google on the name plus keywords from the application area throws up the project web site in the first page of matches.	
Project/software has a distinct name regardless of its application area. A search by Google on the name plus keywords from the application area throws up the project web site in the first page of matches.	
Project/software name does not throw up embarrassing “did you mean…” hits on Google.	
Project/software name does not violate an existing trade-mark.	
Project/software name is trade-marked.	

Copyright To what extent is it clear who wrote the software and owns its copyright?	**Yes/No, supporting comments if warranted**
Web site states copyright.	
Web site states who developed/develops the software, funders etc.	
If there are multiple web sites then these all state exactly the same copyright, licencing and authorship.	
Each source code file has a copyright statement.	
If supported by the language, each source code file has a copyright statement embedded within a	

constant.	
Each source code file has a licence header.	

Licencing Has an appropriate licence been adopted?	**Yes/No, supporting comments if warranted**
Web site states licence.	
Software (source and binaries) has a licence.	
Software has an open source licence.	
Software has an Open Software Initiative[8] (OSI)-recognised licence.	

Governance To what extent does the project make its management, or how its software development is managed, transparent?	**Yes/No, supporting comments if warranted**
Project has defined a governance policy.	
Governance policy is publicly available.	

Community To what extent does/will an active user community exist for this product?	**Yes/No, supporting comments if warranted**
Web site has statement of number of users/developers/members.	
Web site has success stories.	
Web site has quotes from satisfied users.	
Web site has list of important partners or collaborators.	
Web site has list of the project's publications.	
Web site has list of third-party publications that	

[8] http://www.opensource.org/

cite the software.	
Web site has list of software that uses/bundles this software.	
Users are requested to cite the project if publishing papers based on results derived from the software.	
Users are required to cite a boilerplate citation if publishing papers based on results derived from the software.	
Users exist who are not members of the project.	
Developers exist who are not members of the project.	

Accessibility To what extent is the software accessible?	**Yes/No, supporting comments if warranted**
Binary distributions are available (whether for free, payment, registration).	
Binary distributions are freely available.	
Binary distributions are available without the need for any registration or authorisation of access by the project.	
Source distributions are available (whether for free, payment, registration).	
Source distributions are freely available.	
Source distributions are available without the need for any registration or authorisation of access by the project.	
Access to source code repository is available (whether for free, payment, registration).	
Anonymous read-only access to source code repository.	
Ability to browse source code repository online.	
Repository is hosted externally to a single organisation/institution in a sustainable third-	

party repository (e.g. SourceForge, GoogleCode, LaunchPad, GitHub) which will live beyond the lifetime of any current funding line.	
Downloads page shows evidence of regular releases (e.g. six monthly, bi-weekly, etc.).	

Testability How straightforward is it to test the software to verify modifications?	**Yes/No, supporting comments if warranted**
Project has unit tests.	
Project has integration tests.	
For GUIs, project uses automated GUI test frameworks.	
Project has scripts for testing scenarios that have not been automated (e.g. for testing GUIs).	
Project recommends tools to check conformance to coding standards.	
Project has automated tests to check conformance to coding standards.	
Project recommends tools to check test coverage.	
Project has automated tests to check test coverage.	
A minimum test coverage level that must be met has been defined.	
There is an automated test for this minimum test coverage level.	
Tests are automatically run nightly.	
Continuous integration is supported – tests are automatically run whenever the source code changes.	
Test results are visible to all developers/members.	
Test results are visible publicly.	

Test results are e-mailed to a mailing list.	
This e-mailing list can be subscribed to by anyone.	
Project specifies how to set up external resources e.g. FTP servers, databases for tests.	
Tests create their own files, database tables etc.	

Portability To what extent can the software be used on other platforms?	**Yes/No, supporting comments if warranted**
Application can be built on and run under Windows.	
Application can be built on and run under Windows 7.	
Application can be built on and run under Windows XP.	
Application can be built on and run under Windows Vista.	
Application can be built on and run under UNIX/Linux.	
Application can be built on and run under Solaris.	
Application can be built on and run under RedHat.	
Application can be built on and run under Debian.	
Application can be built on and run under Fedora.	
Application can be built on and run under Ubuntu.	
Application can be built on and run under MacOSX.	
Browser applications run under Internet Explorer.	
Browser applications run under Mozilla Firefox.	
Browser applications run under Google Chrome.	
Browser applications run under Opera.	

Browser applications run under Safari.	

Supportability To what extent will the product be supported currently and in the future?	**Yes/No, supporting comments if warranted**
Web site has page describing how to get support.	
User doc has page describing how to get support.	
Software describes how to get support (in a README for command-line tools or a Help=>About window in a GUI).	
Above pages/windows/files describe, or link to, a description of “how to ask for help” e.g. cite version number, send transcript, error logs etc.	
Project has an e-mail address.	
Project e-mail address has project domain name.	
E-mails are read by more than one person.	
E-mails are archived.	
E-mail archives are publicly readable.	
E-mail archives are searchable.	
Project has a ticketing system.	
Ticketing system is publicly readable.	
Ticketing system is searchable.	
Web site has site map or index.	
Web site has search facility.	
Project resources are hosted externally to a single organisation/institution in a sustainable third-party repository (e.g. SourceForge, GoogleCode, LaunchPad, GitHub) which will live beyond the lifetime of the current project.	
E-mail archives or ticketing system shows that queries are responded to within a week (not necessarily fixed, but at least looked at and a	

decision taken as to their priority).	
If there is a blog, is it is regularly used.	
E-mail lists or forums, if present, have regular posts.	

Analysability How straightforward is it to analyse the software's source release to: • To understand its implementation architecture? • To understand individual source code files and how they fit into the implementation architecture?	**Yes/No, supporting comments if warranted**
Source code is structured into modules or packages.	
Source code structure relates clearly to the architecture or design.	
Project files for IDEs are provided.	
Source code repository is a revision control system.	
Structure of the source code repository and how this maps to the software's components is documented.	
Source releases are snapshots of the repository.	
Source code is commented.	
Source code comments are written in an API document generation mark-up language e.g. JavaDoc or Doxygen.	
Source code is laid out and indented well.	
Source code uses sensible class, package and variable names.	
There are no old source code files that should be handled by version control e.g. "SomeComponentOld.java".	
There is no commented out code.	

There are no TODOs in the code.	
Auto-generated source code is in separate directories from other source code.	
How to regenerate the auto-generated source code is documented.	
Coding standards are recommended by the project.	
Coding standards are required to be observed.	
Project-specific coding standards are consistent with community or generic coding standards (e.g. for C, Java, FORTRAN etc.).	

Changeability How straightforward is it to modify the software to: • Address issues? • Modify functionality? • Add new functionality?	**Yes/No, supporting comments if warranted**
Project has defined a contributions policy.	
Contributions policy is publicly available.	
Contributors retain copyright/IP of their contributions.	
Users, user-developers and developers who are not project members can contribute.	
Project has defined a stability/deprecation policy for components, APIs etc.	
Stability/deprecation policy is publicly available.	
Releases document deprecated components/APIs in that release.	
Releases document removed/changed components/APIs in that release.	
Changes in the source code repository are e-mailed to a mailing list.	
This e-mailing list can be subscribed to by anyone.	

Evolvability To what extent will the product be developed in the future: • For a future release? • Within a roadmap for the product?	**Yes/No, supporting comments if warranted**
Web site describes project roadmap or plans or milestones (either on a web page or within a ticketing system).	
Web site describes how project is funded/sustained.	
Web site describes end dates of current funding lines.	

Interoperability To what extent does the software's interoperability: • Meet appropriate open standards? • Function with required third-party components? • Function with optional third-party components?	**Yes/No, supporting comments if warranted**
Uses open standards.	
Uses mature, ratified, non-draft open standards.	
Provides tests demonstrating compliance to open standards.	

Appendix 3 – Questionnaire for usage of models and hypermodels in the clinical setting

This questionnaire is developed to get feedback from all participants of the CHIC project about requirements for the usage of models and hypermodels in the clinical setting.

1. **To which group of stakeholders do you belong?**

   - O Clinician
   - O Software developer
   - O Modeller
   - O Lawyer
   - O System biologist
   - O Geneticist
   - O Bioinformatician
   - O other, please specify: ……

2. **How long do you work in the above-mentioned profession?**

   - O Less than 1 year
   - O 1 – 5 years
   - O 5 – 10 years
   - O 10 – 20 years
   - O > 20 years

3. **What are most important features of models and hypermodels that will foster the usage in the clinical setting? Please rank each item between 1 (not important) and 5 (very important)**

	1	**2**	**3**	**4**	**5**
Clinical relevance	O	O	O	O	O
Usability	O	O	O	O	O
Validation	O	O	O	O	O
Reproducibility	O	O	O	O	O
Reliability	O	O	O	O	O
Certification	O	O	O	O	O
Legal framework to share data	O	O	O	O	O
Models and hypermodels are open source tools	O	O	O	O	O
They can be used after the end of the CHIC project	O	O	O	O	O
There is continuous support for each of them	O	O	O	O	O

4. How do you define clinical relevance?

……

……

……

……

……

5. How important are IP issues of models and hypermodels? Please rank them between 1 (not important) and 5 (very important)

	1	2	3	4	5
For developers	O	O	O	O	O
For end-users	O	O	O	O	O

6. How to convince clinicians to use models and hypermodels? Please rank each item between 1 (not important) and 5 (very important)

	1	2	3	4	5
Writing scientific papers in clinical journals	O	O	O	O	O
Demonstrating models and hypermodels on clinical conferences	O	O	O	O	O
Running workshops for clinicians demonstrating models and hypermodels	O	O	O	O	O
Creating teaching material about models and hypermodels	O	O	O	O	O
Developing eLearning tools for teaching purposes	O	O	O	O	O
Guaranteeing data safety and security	O	O	O	O	O
Running clinical trials by using of models and hypermodels like trials for drug approval	O	O	O	O	O

7. **How to validate the nephroblastoma scenario?**

……

……

……

……

……

8. **How to validate the glioblastoma scenario?**

……

……

……

……

……

9. **How to validate the lung cancer scenario?**

……

……

……

……

……

10. How to validate the prostate cancer scenario?

……

……

……

……

……

11. Are you aware of the ISO (International Organization for Standardization, http://www.iso.org/iso/home.html) SQuaRE (Software product Quality Requirements and Evaluation) and its standards (General Guidance: ISO/IEC 25000, Particular Guidance: ISO/IEC 25040 (ISO/IEC 9126-1 and ISO/IEC 14598-1) and Execution: ISO/IEC 25041 (ISO/IEC 14598-6), ISO/IEC 25042 (ISO/IEC 14598-3), ISO/IEC 25043 (ISO/IEC 14598-4)?

O yes

O no

12. Shall these standards be used as a reference model?

O yes

O no

O do not know

13. How important are the following external and internal quality criteria? Please rank each item between 1 (not important) and 5 (very important)

	1	**2**	**3**	**4**	**5**
Functionality	O	O	O	O	O
Suitability	O	O	O	O	O
Accuracy	O	O	O	O	O
Interoperability	O	O	O	O	O
Security	O	O	O	O	O
Compliance	O	O	O	O	O

Reliability	O	O	O	O	O
Maturity	O	O	O	O	O
Fault tolerance	O	O	O	O	O
Recoverability	O	O	O	O	O
Compliance	O	O	O	O	O
Usability	O	O	O	O	O
Understandability	O	O	O	O	O
Learnability	O	O	O	O	O
Operability	O	O	O	O	O
Attractiveness	O	O	O	O	O
Compliance	O	O	O	O	O
Efficiency	O	O	O	O	O
Time behaviour	O	O	O	O	O
Resource	O	O	O	O	O
Utilization	O	O	O	O	O
Compliance	O	O	O	O	O
Maintainability	O	O	O	O	O
Analysability	O	O	O	O	O
Changeability	O	O	O	O	O
Stability	O	O	O	O	O
Testability	O	O	O	O	O
Compliance	O	O	O	O	O
Portability	O	O	O	O	O
Adaptability	O	O	O	O	O
Installability	O	O	O	O	O
Co-existence	O	O	O	O	O
Replaceability	O	O	O	O	O
Portability	O	O	O	O	O
Compliance	O	O	O	O	O

The questionnaire could be answered online using the following link:

https://docs.google.com/forms/d/1UpF81vGIgqtNBx1x57X1fez6GF0SpD2OmwJSlJGvDV0/viewform?usp=mail_form_link

Appendix 4 – Evaluation and Validation Protocol Template (Version 0.1)

Purpose

The purpose of this document is to specify the validation process to ensure that the CHIC platform with its related functionalities meet the specifications and intended use. The CHIC project aims at developing cutting edge ICT tools, services and secure infrastructure to foster the development of elaborate and reusable integrative models (hypermodels) and larger repositories so as to demonstrate benefits of having both the multiscale data and the corresponding models readily available.

This report presents a template to support evaluators to standardize the clinical adaptation and validation process including standardized reports. It will suggest possible improvements, modifications and other functionalities to the technical WPs in a feedback loop.

General Validation Check-List

The general validation check-list has been adapted from the Annex 11 of the EudraLex, The Rules Governing Medicinal Products in the European Union, Volume 4, Good Manufacturing Practice, Medicinal Products for Human and Veterinary Use.

Requirement	Yes/No, supporting comments
Risk Management Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality.	
Personnel All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.	
Suppliers and Service Providers When third parties (e.g. suppliers, service providers) are used e.g. 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.	
Validation The validation documentation and reports should cover the relevant steps of the lifecycle.	
Data Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.	
Printouts It should be possible to obtain clear printed copies of electronically stored data	
Audit Trails Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail").	

Periodic evaluation Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP	
Security • Physical and/or logical controls should be in place to restrict access to computerized system to authorised persons. 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. • The extent of security controls depends on the criticality of the computerised system. • Creation, change, and cancellation of access authorisations should be recorded. • Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.	
Incident Management All incidents, not only system failures and data errors, should be reported and assessed.	
Electronic Signature Electronic records may be signed electronically	
Business Continuity 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 (e.g. a manual or alternative system).	
Archiving Data may be archived.	

Criteria-Based Assessment

A criteria-based assessment gives a measurement of quality and is derived from ISO/IEC 9126-1 Software engineering - Product quality. This check list is adapted from the Software Evaluation Guide elaborated by Mike Jackson, Steve Crouch and Rob Baxter from The Software Sustainability Institute.

Requirements		Yes/No, supporting comments
Usability		
	Understandability Easily understood?	
	Documentation Comprehensive, appropriate, well-structured user documentation?	
	Buildability	

	Straightforward to build on a supported system?
	Installability Straightforward to install on a supported system?
	Learnability Easy to learn how to use its functions?
Sustainability and maintainability	
	Identity Project/software identity is clear and unique?
	Copyright Easy to see who owns the project/software?
	Licencing Adoption of appropriate licence?
	Governance Easy to understand how the project is run and the development of the software managed?
	Community Evidence of current/future community?
	Accessibility Evidence of current/future ability to download?
	Testability Easy to test correctness of source code?
	Portability Usable on multiple platforms?
	Supportability Evidence of current/future developer support?

Analysability Easy to understand at the source level?	
Changeability Easy to modify and contribute changes to developers?	
Evolvability Evidence of current/future development?	
Interoperability Interoperable with other required/related software?	

GCP Validation Questionnaire

Good Clinical Practice (GCP) is an international ethical and scientific quality standard for designing, recording and reporting trials involving human subject participation. GCP validation questionnaire has been selected from the reported results of p-medicine project.

Requirement	Yes/No, supporting comments
Is a conventional or agile approach used for software development?	
Organisation of the agile approach (for example, exist product owner, scrum master, meeting schedule)	
Does a software development plan (SDP) exist?	
Do developers participate in training?	
Are members of the software group trained to perform their development activities?	
Do SOPs for the development activities exist?	
Existence of an information security policy (ICP)	
Information security awareness, education and training	
Do developers have knowledge/experience with testing and validation of computer systems (e.g. previous audits, inspections)?	
Reports of previous audits or inspections	

Familiarity of developers with the regulatory background for software for clinical research (e.g. GCP)
Is software developed /maintained/adapted according to SDLC (system development life-cycle)?
Use of development standards
Are written policies in place and employed for document review?
Is there a unique definition, which documents underlie a review process?
How is the review process organized?
Are processes for deviations specified?
Is system documentation that covers system architecture, individual modules / classes and their inputs, outputs, and purposes developed that can be provided?
Reference installations for separate phases: e.g. initial installation, then test phase use and routine use
Are written policies in place and employed for integrity tests, security checks, patches and updates that are security relevant?
Are written policies in place for emergency precautions?
Software Quality Assurance (SQA) activities
Review of Software Quality Assurance (SQA) activities by management
Are software quality assurance activities trained?
SQA review of the activities and developed products of the group
Written policy for managing requirements
Written policy for managing the software project
Written policy for software configuration management
Written policy for employing and maintaining a standard software development process
Written policy for training

Written policies for a developer audit by ECRIN
Are adequate resources provided for quality management activities?
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?
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?
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
Testing of the software tools
Testing done by a dedicated and independent person/group
Written policies in place and employed for the test activities?
Risk-based testing? (Risk based testing uses risk to prioritize the appropriate test cases)
Do you test according to risks of GCP relevance (e.g. risks for patient's wellbeing)?
Software Quality Control / Testing Plan
Is the testing done in a systematic way?
Separation of development, test and operational activities exist
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.
Systematic approach to the specification of the amount of testing
Evaluators/reviewers are different persons than the developers
Definition, from which change on a re-testing, completely or partly, is necessary
Definition of responsibilities for change management (release of change, implementer, reviewer)
Are SOPs for using the tool (system) available and maintained?
A security system maintained that prevents unauthorized access to the data?
A list is maintained of the individuals who are authorized to make data changes
Allows the tool direct access to source data/documents for trial-related monitoring, audits, IRB/IEC review, and regulatory inspection?
Requirements documentation (e.g. functional requirements) can be provided to support system validation
Test documentation can be provided to support system validation
Can test reports be provided to support system validation?
Test reviews, including document reviews, performed in the different phases of tool development (IQ, OQ, PQ)
Does the developer or another p-medicine group perform system validation of the developed software?
Do test reports exist that can become part of the validation plan?
Access control policy exist
User access management and user registration exist
Does a policy for user password management exist?

Decisions on the extent of validation and data integrity controls are based on a justified and documented risk assessment of the system
Can close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT personal be shown?
Is it assured that the competence and reliability of a supplier are key factors when selecting a product or service provider?
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?
Listing of all relevant systems / components and their GXP functionality
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
User Requirements Specifications describe the required functions of the computerised system and are they based on a documented risk assessment of GXP impact.
Is the customised computerised system formally assessed and are quality and performance measures for all the life-cycle stages of the system reported?
Demonstration of evidence for appropriate test methods and test scenarios. Are system (process) parameter limits, data limits and error handling considered?
Risk management of the tools that cover the criticality and the potential consequences of erroneous or incorrectly entered data
Is data secured by both physical and electronic means against damage?
Is stored data checked for accessibility, readability and accuracy? Can the access to data be ensured throughout the retention period?
Regular back-ups of all relevant data
Is the integrity and accuracy of back-up data and the ability to restore the data checked?
Obtain clear printed copies of electronically

stored data	
For records supporting batch release, is it possible to generate printouts indicating if any of the data has been changed since the original entry?	
Are audit trails available and convertible to a generally intelligible form and regularly reviewed?	
Are any changes to a computerised system including system configurations only possible in a controlled manner in accordance with a defined procedure?	
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).	
Physical and/or logical controls are in place to restrict access to computerised system to only authorised persons	
Does the extent of security controls depend on the criticality of the computerised system?	
Are the creation, change, and cancellation of the access authorizations recorded?	
Are all incidents, not only system failures and data errors, reported and assessed?	
Are electronic records signed electronically (e.g. password)?	
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?	
Is archived data checked for accessibility, readability and integrity?	
If relevant changes are made to the system, is the ability to retrieve the data ensured and tested?	

Clinical Scenarios Validation

Cancer Hypermodel Usability Check-List

Requirement	Yes/No, supporting comments

	Hypermodel for Nephroblastoma	Hypermodel for Glioblastoma	Hypermodel for Non-Small-Cell Lung Cancer (NSCLC)	Hypermodel for prostate cancer
How straightforward is it to understand: • What the hypermodel does and its purpose? • The intended market and users of the software? • The software's basic functions? • The software's advanced functions?				
High-level description of what/who the hypermodel is for is available.				
High-level description of what the hypermodel does is available.				
High-level description of how the hypermodel works is available.				
Design rationale is available - why it does it the way it does.				
Architectural overview, with diagrams, is available.				
Descriptions of intended use cases are available.				
Case studies of use are available.				

CHIC Portal Functionalities Check-List

Requirement	Yes/No, supporting comments
CHIC portal and user registration frames The interfaces which allow a user to access a CHIC services	
CHIC identity provider (IDP)	
CHIC Trusted Third Party (TTP) De-Identification and Upload of data into the CHIC platform	
Models and Hypermodels Access to reusable integrative models (hypermodels) and larger repositories	
Sematic annotation The presence of semantic annotation frames	
Data flow and integration Data flow and data integration interfaces according to specific data types	

Wilms Tumor Scenario Validation

Requirement	Yes/No, supporting comments
Scenario description	**Yes** D2.2 - Scenario based user needs and requirements (Chapter 5. Scenarios for Nephroblastoma): • Clinical scenario • Imaging scenario • Molecular scenario • Validation scenario • Machine learning scenario • Advanced Nephroblastoma scenario • Drug selection scenario
Available data The availability of retrospective and prospective data: • Clinical data • Pathological data • Imaging data • Molecular data	
Hypermodel Usability Check-List (Chapter 5.1)	
Validation Protocol	**Yes** The validation protocols is based on the “Evaluation and Validation Protocol Template”
Usage Survey Questionnaire for usage of models and hypermodels in the clinical setting	

Glioblastoma Multiforme Scenario Validation

Requirement	Yes/No, supporting comments
Scenario description	**Yes** D2.2 - Scenario based user needs and requirements (Chapter 6. Scenarios for Glioblastoma): • Clinical scenario • Imaging scenario • Molecular scenario • Radio- and chemotherapy scenario • Immunotherapy scenario • Validation scenario • Machine learning scenario
Available data The availability of retrospective and prospective data: • Clinical data • Pathological data (Tumor characteristics) • Imaging data • Data inherent to the HGG-2010 protocol outline • Monitoring data • Molecular data	
Hypermodel Usability Check-List (Chapter 5.1)	
Validation Protocol	**Yes** The validation protocols is based on the “Evaluation and Validation Protocol Template”
Usage Survey Questionnaire for usage of models and hypermodels in the clinical setting	

Non-Small Cell Lung Cancer Scenario Validation

Requirement	Yes/No, supporting comments
Scenario description	**Yes** D2.2 - Scenario based user needs and requirements (Chapter 7. Scenarios for Non-Small-Cell Lung Cancer (NSCLC)): • Clinical scenario • Imaging scenario • Molecular scenario • Drug selection scenario • Validation scenario • Machine learning scenario
Available data The availability of retrospective and prospective data: • Clinical data • Pathological data (Tumor characteristics) • Imaging data • Molecular data • Data inherent to the HGG-2010 protocol outline • Monitoring data • Molecular data	

Hypermodel Usability Check-List (Chapter 5.1)	
Validation Protocol	**Yes** The validation protocols is based on the "Evaluation and Validation Protocol Template"
Usage Survey Questionnaire for usage of models and hypermodels in the clinical setting	

Other Cancer Types Scenario Validation

Requirement	Yes/No, supporting comments
Scenario description	**Yes** D2.2 - Scenario based user needs and requirements (Chapter 8. Scenarios for prostate cancer): • Clinical scenario • Imaging scenario • Molecular scenario • Drug selection scenario • Validation scenario • Machine learning scenario
Available data The availability of retrospective and prospective data: • EUREKA-1 Data • EUREKA-2 Data	
Hypermodel Usability Check-List (Chapter 5.1)	
Validation Protocol	**Yes** The validation protocols is based on the "Evaluation and Validation Protocol Template"
Usage Survey Questionnaire for usage of models and hypermodels in the clinical setting	

Evaluation and Validation Protocol

Validation Activity	Performed by	Date	Signature
General Validation Check-List			
Criteria-Based Assessment			
GCP Validation Questionnaire			
Cancer Hypermodel Usability Check-List			
CHIC Portal Functionalities Check-List			
Wilms Tumor Scenario Validation			
Glioblastoma Multiforme Scenario Validation			
Non-Small Cell Lung Cancer Scenario Validation			
Other Cancer Types Scenario Validation			