Giving patients a voice

Evaluation Software Development Policy Manual

Evaluation Software Development (ESD)
Valiergasse 60-62
A-6020 Innsbruck
E-Mail: office@ches.pro
Version 7.0, September 2020.

Contents

1 Introduction 1
1.1 The mission of ESD . . . 1
1.2 Usage scenarios of CHES . . . 2
1.3 Revision History . . . 5

2 Policies 7
2.1 System Implementation . . . 7
2.2 Data Privacy . . . 13
2.3 Data Security . . . 17
2.4 Data Archival . . . 21

Glossary 24

Bibliography 25

Appendix 26
Terms and Conditions . . . 26

Chapter 1

Introduction

The company Evaluation Software Development (ESD), founded as an academic spin-off in 2005, focuses on the development of medical IT solutions for use in research projects, quality assurance, and daily clinical routine. The software products are utilized for collection and graphical presentation of medical and Patient Reported Outcomes (PROs) data. ESD provides innovative, high-quality technical solutions in the field of PROs, enabling clients to achieve their full potential in their contributions to the global medical and scientific community.

The company ESD has been developing PRO software products since 2005. The software Computer-Based Health Evaluation System (CHES), the main software product of ESD, provides a sophisticated graphical user interface allowing easy access to PRO profiles of individual patients. To date, the software has been used at hospitals and research institutions all over the world, e.g., in Austria, Australia, Belgium, Canada, China, Czech Republic, France, Germany, India, Italy, Japan, Kuwait, Spain, South Korea, Switzerland, UK, US and more — with far more than a million assessments performed up to now. Currently, ESD is involved in numerous research projects funded by EU, EORTC, GIMEMA, Austrian Children's Cancer Aid, Austrian National Bank, Austrian Science Fund (FWF), The Austrian Research Promotion Agency (FFG) and Tyrolean Health Fund. Furthermore, CHES is also applied in other fields of medicine besides oncology such as orthopedics, neurology, rehabilitation and cardiology. In recent years ESD has considerably expanded their product portfolio. For clinical trials ESD has developed a modern, validated and, above all, cost-effective Clinical Trial Management System (CTMS), specifically for small and medium-sized pharmaceutical companies. The CTMS with Case ReportForm (eCRF), Trial Master File (eTMF), Investigator Site File (eISF), and the Feasibility Tool is extended by further useful tools such as Milestones, Budgeting, etc.

1.1 The mission of ESD

The mission of our team is to develop, deliver and maintain software that truly satisfies the needs of our clients. We have learned in years of developing innovative software for academia and industry that innovative and custom–made software cannot just be described in the form of a written document and then "simply" turned into software. Rather, we see software development as an ongoing discussion between our team and our clients. To achieve and operationalize respective processes, our development processes are based on agile software development. The iterative nature of agile development allows for features that are delivered incrementally, enabling benefits to be realised early as the product continues to develop. Our key principles that build the basis for implementations (cf. Section 2.1) can be described as follows:

- *Quality.* A key principle of agile development is that testing is integrated throughout the lifecycle, enabling regular inspection of the working product as it develops. This allows the product owner to make adjustments if necessary and gives the product team early sight of any quality issues. Automated testing of our software by unit tests ensures the technical quality of our products.
- *Visibility.* Development principles of agile software development encourage active user involvement throughout the product's development in a very cooperative, collaborative way. This provides excellent visibility for key stakeholders, both of the project's progress and of the product itself, which in turn helps to ensure that expectations are effectively managed. Early prototypes are constantly made available, allowing for externally monitoring the project's progress. Our clients receive access to our issue tracking system (Redmine), which gives additional insights into the project's progress.
- *Risk Management.* Small incremental releases visible to the product owner and product team through its development help to identify any issues early and make it easier to respond to change. The clear visibility in agile development helps to ensure that any necessary decisions can be taken at the earliest possible opportunity, while there's still time to make a material difference to the outcome. In all our development efforts, we analyze potential risks of the projects. By delivering early prototypes, risk related to performance or maintenance can be detected early and mended early, minimizing the cost of changes. Similarly, risk with respect to cost overrun or misinterpretation of requirements can be detected early and respective countermeasures can be applied.
- *Change Management.* As direct consequence of the agile development process, change and respective change management activities are in the core of our efforts.

Since our development processes are based on agile software development, we have established an agile company culture since the academic spin-off ESD was founded in 2005. A central tenet of the agile movement is the requirement for highly skilled developers. Since agile teams are expected to be small, self-governing and self-regulated, there is a high expectation in regard to the personal attributes of team members. They should enjoy the special challenges of working in an agile environment, be prepared to forego personal recognition in favor of team accomplishment and enjoy working in a highly transparent environment in which their work products, creativity and diligence are visible to their teammates and clients. All of our employees have an academic degree, are very enthusiastic and appreciate the work-life balance in our company. A result of these facts is that the core team of software developers and researcher are part of ESD since the very beginning.

1.2 Usage scenarios of CHES

CHES, a software product of ESD, is based on a modular architecture that allows for the customization of CHES for a variety of usage scenarios. In this document, we distinguish between two standard scenarios as detailed subsequently, since the respective scenarios impact the the applicability of the policies. Deviations from these scenarios are also supported by ESD, but must be evaluated for each client specifically.

1.2.1 Modules of CHES

CHES is not a single application, but a set of modules, each specifically designed for their respective use cases. Subsequently, the modules of CHES are briefly introduced.

- CHES.Main: CHES.Main is the main application of the system, which is used for managing patients, recording patient data, planning and managing the assessment of questionnaires, and the management of the patients' studies. The patients' questionnaire results are processed and presented to the user as charts. CHES.Main is also responsible for interacting with other applications in the client's IT infrastructure via its interfaces, e.g,. HL7.

- CHES.Nurse: When developing CHES.Nurse, the aim was to create a light-weight application for tablets, specifically focused on administering questionnaires. In a typical usage scenario a study nurse would be visiting their patients in their hospital rooms to complete their daily questionnaire.

- CHES.Admin: If a user has the appropriate privileges, CHES.Admin can be used to configure the CHES installation. This includes administrative settings like the creation of users and their privileges, or the configuration of patient lists. Additionally, clinical settings, e.g., reference values for the interpretation of questionnaire results, can be configured.

- CHES.Portal: The applications mentioned before are all intended to be used while a patient is present at the hospital. CHES.Portal (and its predecessor CHES.Home) try to alleviate the patient from the burden of coming to the hospital to complete a questionnaire. With CHES.Portal, patients can complete their questionnaires from anywhere using their own desktop computers, tablets, or mobile phones. Additionally, CHES.Portal comes with a full-fledged website, allowing our clients to provide tailored content specific to the patients' disease.

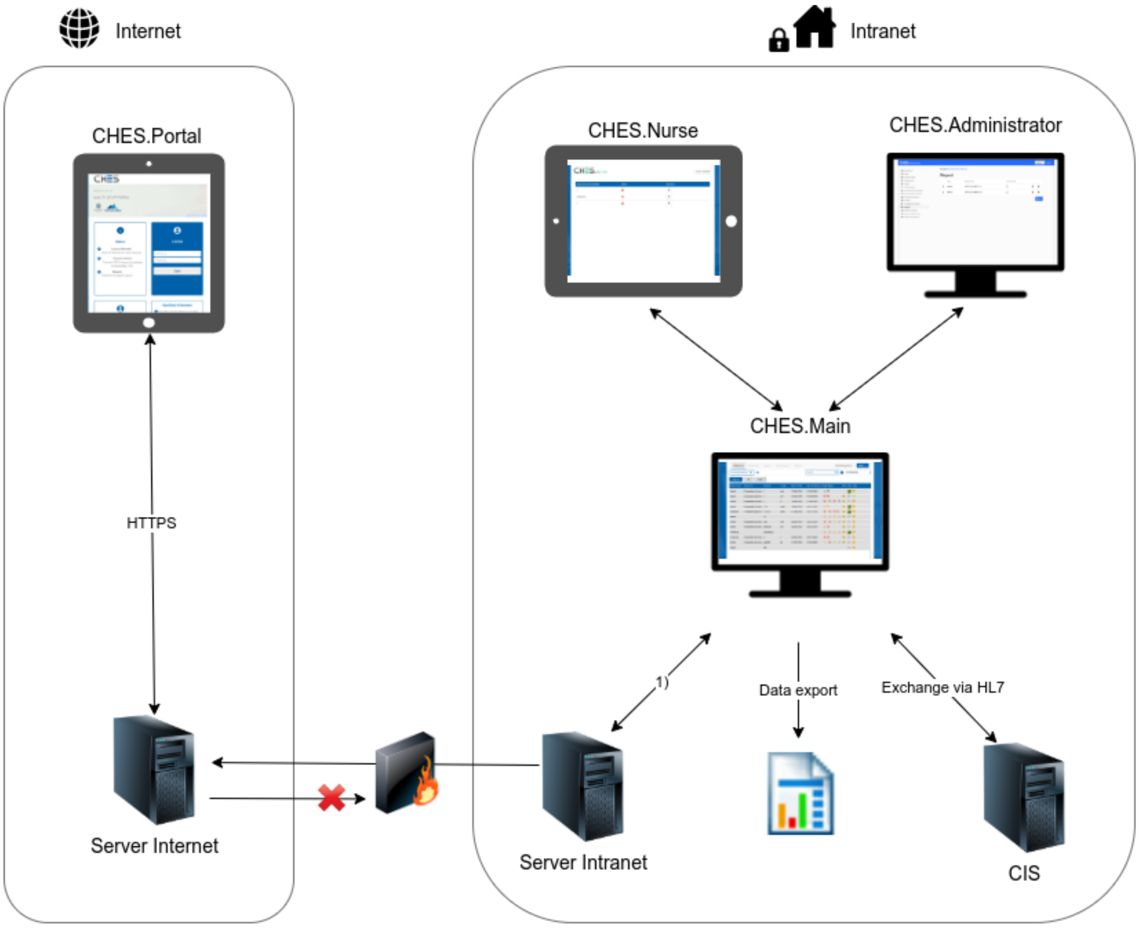
- CHES.Portal-Admin: CHES.Portal is complemented with a content management system, which allows our clients to adapt the content displayed to the patients.

1.2.2 Scenario 1. Daily clinical routine: CHES running in the client's private network

This scenario describes a typical setting for using CHES in daily clinical routine or for clinical trials conducted by a single research institution. In such scenarios, CHES might be required to interact with the clinical information system and therefore be capable of handling personal identifiable data. As a result, the CHES software has to be installed within the client's private network.

In such usage scenarios, where personal identifiable data is used in CHES, we recommend that the server should not be be a accessible via the Internet. To allow for the usage of

CHES.Portal, which needs to be accessible via the Internet, we recommend a second server for running CHES.Portal that has no access to personal identifiable data (cf. Section 2.2).



1) Also the applications CHES.Nurse and CHES.Administrator communicate with "Server Intranet". This detail was intentionally omitted for the sake of visual clarity.

Figure 1.1: Modules of CHES in a clinical environment

Figure 1.1 illustrates such a usage scenario with respect to the different modules of CHES. Within the private network, the modules of CHES that can access the main database, i.e., CHES.Main, CHES.Nurse, and CHES.Admin, are running. These modules are protected by access control mechanisms to allow access to authorized personnel only.

CHES.Portal (and CHES.Portal-Admin) is running on Server Internet. A synchronization service, running on Server Intranet, is responsible for keeping the two servers in sync while ensuring that no personal identifiable data is transferred to the Internet server. Please note, as indicated by the red cross in Figure 1.1, connections cannot be established from Server Internet, but are only allowed to be established from Server Intranet. All data that is exchanged between these two servers is fully controlled by Server Intranet, i.e., data is *pushed to* Server Internet and *pulled from* Server Internet on demand.

Interoperability of CHES with clincial information systems (CIS)

In order to facilitate the usage of CHES in clinical routine, CHES connects to existing CIS via a variety of different technologies. Subsequently, several supported interfaces are briefly described. Other interfaces might be supported on request.

Most importantly, CIS that implement the Health Level-7 (HL7) standard can interact with CHES by sending and/or receiving the respective messages. Examples of supported HL7 messages are ADT A01 messages for creating new patients, or ADT A08 messages for updating patient data. This way, there is no need for manually entering patient data multiple time across the hospital.

In addition to sending and receiving HL7 message, CHES supports the interaction with other CIS by exchanging generated files via network shares or File Transfer Protocol (FTP) servers. Typically this approach is utilized for sharing generated Portable Document Format (PDF) files, e.g,. questionnaire result reports, with other CIS.

The management of users and privileges can be conducted using Lightweight Directory Access Protocol (LDAP)/Active Directory (AD). CHES allows for assigning roles from an existing LDAPAD system to roles within CHES. Authentication requests are forwarded to the existing LDAP/AD server. Similarly, CHES allows for delegating authentication requests to existing Kerberos (protocol) (Kerberos) systems.

Besides, CHES is capable of sending E-Mail reminders to users and patients. This way, patients who are completing questionnaires from their home can be automatically reminded if they forget to fill out their questionnaire. Custom E-Mail reminders for patients and users can be implemented if required.

1.2.3 Scenario 2. Multi-center clinical trial: CHES running on ESD's servers accessible via the Internet

In contrast to installations for daily clinical routine or smaller clinical trials that are conducted only within one research institution, large, multi-center clinical trials impose different requirements. In such a scenario, it is essential that all participating research institutions have access to the data collection instrument. To accommodate for this requirements, ESD offers the the possibility to host CHES on their servers, making it available to all research institutions.

In such scenarios, all modules can be used. Since the system needs to be accessible via the Internet, additional requirements regarding data privacy, i.e., the storage of personal identifiable data, have to be considered (cf. Section 2.2). Further, interactions with clinical information systems are not possible since such system are usually not accessible via the Internet.

1.3 Revision History

- Gerhard Rumpold (2009-04-16): Version 1.0 of the introduction.
- Gerhard Rumpold (2013-09-01): Version 2.0 of the introduction.
- Jakob Pinggera (2016-05-12): Version 3.0 of the introduction.
- Jakob Pinggera (2018-07-24): Version 4.0 of the introduction.

- Stefan Zugal (2020-08-26): Version 5.0 of the introduction.
- Jakob Pinggera (2020-08-27): Version 6.0 of the introduction.
- Gerhard Rumpold (2020-09-14): Version 7.0 of the introduction.

Chapter 2

Policies

2.1 System Implementation

The quality of data collected during clinical trials or in daily clinical routine depends heavily on the quality of the instrument that is used for data collection. Especially in the context of clinical trials, the collection of the *right* data is essential for their successful analysis. As a consequence, design, development and quality assurance of a data collection instrument must be given the utmost attention [1].

2.1.1 Purpose

This policy is intended to regulate how client specific adaptations of CHES are developed. For this, it describes the process of elicitating requirements for clients, the adaptations of the software, the review process by the client, i.e., user acceptance testing, installation of the software, system maintenance, and, if requested, support during data analysis. For this, this policy is based on “Data Acquisition” described in [1].

This policy focuses on orchestrating client specific adaptations of CHES. Therefore, it does not cover quality assurance mechanisms during the software development development lifecycle, e.g,. automated unit testing, which are conducted by ESD.

2.1.2 Scope

This policy is directed at all employees at ESD who are responsible for the elicitation of requirements and/or the development of client specific adaptation. Further, the policy is of interest for clients, who are interested in acquiring CHES for conducting a clinical trial or for daily clinical routine as their obligations are outlined. Finally, the policy is directed at system administrators of clients, as it regulates how CHES is installed and maintained on the client’s infrastructure.

2.1.3 Policy

This policy is aligned with the different stages of developing the adaptations of the software. As indicated in Section 1, we are following an agile, iterative approach to software development. Therefore, the first three stages listed here, i.e., requirements elicitation, software adaptation, and client review, may be repeated in several iterations, allowing the tailoring of CHES according to the client’s needs.

Requirement elicitation

In a first step, the client is responsible for developing at least a preliminary protocol for a clinical trial or compile a list of intended features if CHES should be used in daily clinical routine. In this context, the client is responsible complying with all regulations, e.g., obtaining ethics approval for a clinical trial.

CHES module selection The list of features/study protocol are then matched by ESD against the standard features provided by CHES. In this context, different scenarios imply the selection of different CHES modules (cf. Section 1.2.1). For example, if data is primarily collected in hospitals, CHES.Nurse, a lightweight tool for data collection on mobile devices, is usually recommended. Similarly, including CHES.Portal might be beneficial in clinical routine as it might increase the number of data points. On the contrary, in clinical trials, the setting that is used for data collection, i.e., at home or in a hospital, might have an impact on the collected data [8]. Therefore, the setup has to be evaluated for each client individually to guarantee the best possible experience for the specific use case.

Patient data selection Additionally required adaptations to the software are identified. Such adaptations usually include patient data variables, e.g., blood pressure, that should be collected. This way, it is ensured that all key variables are collected. By elicitating the requirements with our clients, we can draw from years of experience on how to utilize CHES in clinical trials or in daily clinical routine. For example, ESD is keen to avoid any duplicated entry of data unless absolutely required, utilize pre-defined codings for variables, i.e., combo boxes, instead of free text, or suggest the usage of standardized patient data forms that have been proven to perform flawlessly in the past.

PRO questionnaires selection Similar to patient data, the selection of appropriate PRO instruments is essential for the success of a clinical trial or for applying PRO in daily clinical routine. Based on the requirements of our clients, we strive for selecting the most appropriate questionnaires from a collection of established PRO questionnaires. If a client wishes to develop a specialized questionnaire, we are keen to support the development process with our expertize and via providing the technical means for conducting the corresponding study. The required domain knowledge has to be provided by the client (cf. [8] for guidelines on how to develop a PRO instrument).

By administering a questionnaire using electronic devices, e.g., tablets, we try to combine the best of two worlds. On the one hand, we intend to resemble the corresponding paper–based PRO instrument as closely as possible while still making use of the benefits of electronic data collection. For instance, if subjects are asked to skip a series of questions based on a previous answer, errors might occur [8]. By utilizing electronic means for data collection, errors can be mitigated by presenting only required questions based on the given answers to the subject. This possibility is exploited when presenting subjects with computerized adaptive testing (CAT) questionnaires, where each question is selected based on previous answers of the subject. Similarly, by administering a questionnaire using electronic devices, CHES can offer the possibility to control the number of allowed missing items in PRO questionnaires depending on the clients's requirements. This way, missing data in PRO questionnaires can be minimized.

In this context, it should be considered that changing an instrument from paper to electronic format, might have an impact on the obtained results [8]. To investigate this claim, considerable research has been conducted. In [3], the authors synthesized a total of 65 studies in order to assess the equivalence of computer versions and paper versions of PRO instruments. The authors concluded that extensive evidence indicates that paper–based and computer–based PRO instruments are equivalent [3]. Therefore, we are confident that the questionnaires administered by CHES yield comparable results to paper–based PRO instruments.

Study schema definition Further, in case of a clinical trial, a study definition is usually extracted from the requirements, which is included in CHES in order to facilitate data collection. This way, the execution of a clinical trial can be supported by CHES, ensuring that data is collected at the appropriate points in time as defined in the clinical trial. As a result, potential data loss can be minimized.

Software adaptation

Once the client and ESD have agreed on a set of requirements as a starting point, software adaptation can begin. For this, the requirement specification is transferred to the issue tracking system of ESD, which records all feature requests and bug reports. Together with a version control system, that links all changes to the software to the appropriate issue in the system, all software adaptations can be traced back to the corresponding requirements. All employees at ESD are required to use the issue tracking system in order to document design decisions.

As indicated previously, ESD follows an agile approach to software development. In this context, the availability of clients for clarification whenever problems arise is of paramount importance. Therefore, clients are expected to reply within a timely manner to requests for clarification in order to avoid unnecessary delays during software adaptation.

Finally, the usability of the software is a primary concern at ESD. Therefore, each developer is responsible for making the software as clear and easy to use as possible, e.g., by making questions and prompts as clear as possible. Similarly, the system has to inform users about entered data that does not match the expected data format or it out of the expected range for the data. In this context, the use of default values for patient data that are automatically inserted is strongly discouraged. Further, developers are asked to incorporate the client's workflows into the development of new features to easen their usability.

Client review and user acceptance testing

Agile software development builds upon early feedback by users. For this, CHES is deployed as early as possible on one of ESD's servers and filled with test data, i.e., artificially created data serving solely for the demonstration of the system. The client is asked to access this installation to inspect the adaptations to the system to ensure that all changes result in the intended functionality. The test installation is regularly updated to ensure that an up-to-date version of CHES is available to the client at all times. Once all features are implemented, the client has to inspect the system to ensure that all requirements have been fulfilled. It this is the case, the client has to send a written confirmation to ESD acknowledging that all requirements have been met.

System installation

Once the written confirmation is obtained, ESD installs CHES on the server in the production environment. Depending on the usage scenario (cf. Section 1.2) the following procedures are followed.

Scenario 1. CHES running in the client's private network In case CHES should be running on servers of the the client, ESD will provide the client with a list of requirements, specific to the CHES installation, regarding software that should be installed on the server. System administrators at ESD need to have access to the server in order to set up the system. This is usually accomplished by providing ESD with Virtual Private Network (VPN) access to the server. If required by the client, dedicated privacy agreements might be established between the client and employees at ESD to ensure that no unauthorized data access occurs. In addition, all employees at ESD have to sign a confidentiality agreement before handling any sensitive data (cf. Section 2.2). Once the installation is complete, the client is informed and asked to test the system in the production environment, i.e., access the system from devices that are used for data collection.

Scenario 2. CHES running on ESD's servers accessible via the Internet If CHES is installed on servers of ESD, no information has to be provided by the client. Once the system installation is completed, the client has to test the system from all devices that will be used for data collection.

System maintenance

ESD is responsible for maintaining the CHES installation. For this, support is provided by ESD via phone and e-mail during business hours. Critical problems are handled with highest priority to guarantee a fast and reliable resolution of the problem.

Depending on the usage scenario (cf. Section 1.2), CHES is either installed in the private network of the client or on servers provided by ESD. Further details regarding system maintenance are defined in the general terms and conditions, to be found in Appendix *Terms and Conditions*, Section 8: *Remote Maintenance, Maintenance And Support*. Subsequently, specifics regarding system maintenance in each scenario are outlined.

Scenario 1. CHES running in the client's private network In case CHES is running on servers in the private network of a client, access has to be provided to ESD in order to provide maintenance of the CHES installation. This is usually provided via VPN access as described in system installation.

While ESD is responsible for maintaining the CHES installation, ESD is *not* responsible for the maintenance of the server itself. This means that the client is responsible for setting up and maintaining all infrastructure required for running CHES, including all hardware and software (e.g., server, network, operating system, third party libraries). Similarly, the client is responsible for providing regular backup of data. Also, the installation of system updates need to be conducted by the client and security certificates need to be installed and updated by the client (cf. Section 2.3).

Scenario 2. CHES running on ESD's servers accessible via the Internet In this scenario, ESD is responsible for the maintenance of the CHES installation, but also for the maintenance of the server in terms of hardware and software installed on the server. The client has no responsibilities in terms of system maintenance.

Data analysis

In case of clinical trials, data analysis is usually conducted by researchers without involvement of ESD. Researchers are therefore responsible for appropriate data handling with respect to data privacy, ethical considerations, and integrity of the data analysis. If desired, ESD can support researchers during their analysis by providing dedicated data export mechanisms for the clinical trial at hand.

2.1.4 Related Standards, Policies and Processes

- Data Privacy Policy (cf. Section 2.2)
- Data Archival Policy (cf. Section 2.4)
- Good Clinical Data Management Practices [1]
- Guidance for Industry, Computerized Systems Used in Clinical Investigations (1999) [5]
- Guidance for Industry, Computerized Systems Used in Clinical Investigations (2007) [6]
- Guidance for Industry, Patient-Reported Outcome Measures: Use in Medical Product Development to Support Labeling Claims (2009) [8]

2.1.5 Revision History

- Gerhard Rumpold (2009-04-16): Version 1.0 of the policy.
- Gerhard Rumpold (2013-09-01): Version 2.0 of the policy.
- Jakob Pinggera (2016-05-24): Version 3.0 of the policy.
- Jakob Pinggera (2020-08-27): Version 4.0 of the policy.

2.2 Data Privacy

Data privacy refers to the protection of personal identifiable data. Personal identifiable data can be defined as any information related to a patient in daily clinical routine or a subject in a clinical trial, which can lead to the identification, either directly or indirectly, of that subject. Personal identifiable data might include, but is not limited to, patient names, initials, addresses, and genetic code.

The protection of personal identifiable data is of uttermost importance when developing Case Report Form (CRF)s. This policy was developed based on the data privacy guidelines published in [1].

2.2.1 Purpose

This policy is intended to regulate the storage of personal identifiable data and the corresponding medical data. Further, it regulates the transfer of such data between departments, e.g,. research, development, and between users.

2.2.2 Scope

This policy is directed to all software developers and system administrators working at ESD. Further, the policy is directed to system administrators of clients running the servers where CHES is installed. Further, the policy is directed to user of CHES on how to handle data obtained from CHES. Finally, the policy regulates the data transfer between users of CHES and employees of ESD.

2.2.3 Policy

Storage of personal identifiable data

As described in Section 1.2, CHES can be used in different scenarios, i.e., installed in the client's private network or on servers provided by ESD. As the respective scenario influences the handling of personal identifiable data, the two scenarios are covered explictly.

Scenario 1. CHES running in the client's private network If CHES is used in clinical routine, all modules of CHES accessing the main database (cf. Figure 1.1) have to be set up on servers located at the data center operated by the client. The client is responsible for appropriately securing the physical access to the server (cf. Section 2.3). In this context, personal identifiable data, e.g., the patient's name, can be stored in the database.

If the installation of CHES.Main is accompanied with CHES.Portal/CHES.Home, which need to be accessible via the Internet, CHES.Portal/CHES.Home need to be installed on a separate server that cannot access the main database. Only the minimum required information is synchronized from CHES.Main to the server running CHES.Portal or CHES.Home. This synchronization is always triggered by the server running CHES.Main, as CHES.Portal/CHES.Home cannot initiate a connection to the main database. The synchronized information must not include any information allowing the identification of the subject, with exception of an id that does not allow for any inferences regarding the patient, e.g., patient15.

Scenario 2. CHES running on ESD's servers accessible via the Internet In the context of clinical trials, a CHES installation is usually accessed by researchers from different research institutions. For this, CHES is installed on ESD's servers and therefore accessible via the Internet. In this context, no data allowing the identification of the subject, with exception of an id that does not allow for any inferences regarding the patient, e.g., patient15, is allowed to be stored on the server. If required for the clinical trial, researchers at the participating research institutions are responsible for maintaining a local mapping of patient id to the corresponding patient. This mapping must not be stored in CHES.Main. In this context, ESD is responsible for securing access to the server (cf. Data Security Policy, Section 2.3).

Transfer of patient data between departments

Extra care has be exercised when data is stored and/or transfered outside of CHES. More specifically, CHES.Main allows the export of data for statistical analyses, i.e., in a clinical trial. Once the data is exported, the respective user is responsible to securely storing the data. For this, the exported data should be encrypted and only decrypted for conducting the analysis. Similarly, if data is transferred from one researcher to another, the data has to be encrypted using a state of the art encryption algorithm. ESD will *not* accept any unencrypted data to be transferred via the Internet. For encrypting data, the usage of OpenPGP or any RFC4880-compliant implementation is preferred and strongly recommended by ESD. Thereby, ESD will provide public keys via a recognized public key infrastructure as well as through the website for convenience. To establish the trustworthiness of the keys, clients can rely on the public key infrastructure; additionally ESD offers the possibility for providing key fingerprints via telephone. In case the client is not capable of adopting OpenPGP or any RFC4880-compliant technology, transmitted data must be encrypted using a symmetric state of the art encryption algorithm and the password has to be provided via a different medium than the original data file. For example, if the encrypted data file is transferred via E-mail, the password to decrypt the file could be provided via a personal phone call.

Similarly, it might be necessary to transfer database dumps between servers or from a server to ESD's development team, e.g., to develop a migration routine for a software update. Such database dumps must either be encrypted, as described in the paragraph before, or transfered via a secured connection. Developers at ESD strip the dump from any personal identifiable data before starting to work on the data.

All persons working in the context of CHES, i.e., users, researchers, developers, and system administrators, have to be made aware of this policy prior to start working at ESD or before using CHES. Further, every employee at ESD has to sign a confidentiality agreement before handling any sensitive data.

2.2.4 Related Standards, Policies and Processes

- Data Security Policy (cf. Section 2.3)
- Good Clinical Data Management Practices [1]

2.2.5 Revision History

- Gerhard Rumpold (2009-04-16): Version 1.0 of the policy.
- Gerhard Rumpold (2013-09-01): Version 2.0 of the policy.
- Jakob Pinggera (2016-05-12): Version 3.0 of the policy.
- Jakob Pinggera (2020-08-27): Version 4.0 of the policy

2.3 Data Security

Secure, accessible, and efficient storage of data is paramount for the success of clinical trials specifically and the usage of software systems in daily clinical routine in general. In the context of systems recording their data electronically, this results in distinct requirements for securing the servers that are used for data collection. This policy was developed based on the data storage guidelines published in [1].

2.3.1 Purpose

This policy is intended to regulate the conditions for physically and logically accessing the data stored at the server underlying CHES. In this context, physical access describes the access by technicians that are able to work on the server, i.e., push a button on the machine. Logical security, in contrast, describes access to the server via a network connection. Further, this policy regulates the monitoring of CHES installations and measures that need to be in place in order to recover from potential disasters.

2.3.2 Scope

This policy is intended for developers and system administrators at ESD, but also for system administrators of clients, who might host CHES on servers in their private network.

2.3.3 Policy

Physical Server Security

As described in Section 1.2, CHES can be utilized in different scenarios. In the context of physical server security, the responsibilities change depending on who hosts the CHES installation.

Scenario 1. CHES running in the client's private network If CHES is installed within a client's private network using a database server that is provided by the IT department of the client, physical server security falls within the responsibility of the client.

Scenario 2. CHES running on ESD's servers accessible via the Internet If CHES is installed of ESD's servers, ESD is responsible for securing the physical access to the server. In order to guarantee the constant availability of CHES, ESD relies on servers hosted in a European data center (unless requested otherwise by a client). The data center is responsible for securing access to the data center itself via appropriate mechanisms, e.g., access gates. Further, the server is physically separated and secured from the remaining data center. In case of technical problems, a service technician can be appointed by ESD to complete the required maintenance. The maintenance is recorded on video to ensure that no unintended changes are made to the server. Further, the data center is not allowed to access the server without direct order from ESD. This way, it is ensured that no unauthorized physical access to the server occurs.

Logical Server Security

In addition to physical access to server, logical access, i.e., access via a network connection, has to be secured. For this firewalls have to be in place preventing any unauthorized connections to the server.

In order to use CHES, users are identified by a combination of username and password. CHES does not store any passwords, but computes and stores hash values for passwords, which are used for user authentication. Users might be created and deactivated by users with appropriate privileges using CHES.Admin. Users are not allowed to "share" accounts. Each individual must have their own account. Passwords must consist of at least 8 characters and contain at least one digit. The system must prohibit any password changes that do not comply with this policy. If a logged–in user is idle for a long period, the user has to be logged off automatically. Unsuccessful login attempts are recorded by the system. After a series of unsuccessful login attempts, the utilized device can be blocked for a configurable duration, e.g., CHES could be configured to block the used computer for 60 minutes.

The connection with the server has to be appropriately secured using an encrypted connection, i.e., Hypertext Transfer Protocol Secure (https), Secure Shell (ssh). The identity of the server has to be verified using an appropriate certificate signed by a trusted certification authority. If the server is owned by ESD, ESD is responsible for installing and renewing the certificate. If the server is part of a client's infrastructure, the client is responsible for installing and renewing the certificate.

Audit Trails of Data Entry

In order to allow for the traceability of all changes to the stored data, an audit trail system that records the originator, date and time, including timezone, of the change, and details on the change has to be in place. In case of modifications to previously entered data, the system might force the user add a reason for the change, e.g., transcription error, (depending on the client's requirements). In case of direct entry of data (cf. [9]), the authenticated user is the originator of the audit trail entry. If the data is transmitted via an external system, e.g., a clinical information system via HL7, the external system should be the originator. In case of data entry by a subject/patient, which is usually the case for PRO data, the originator should be the patient.

The audit trail system must log all changes to the state of the system automatically. Additionally, the system must allow for manual additions to the audit trail in case system administrators of ESD have to interfere with the system directly. This functionality is only available to employees of ESD and should only be used as a last resort.

The audit trail log has to be secured appropriately, i.e., encrypted or using an access control mechanism. If requested, system administrators at ESD can provide authorized personnel with an export of the audit trail.

Server Monitoring and Disaster Recovery

ESD is responsible for monitoring servers located in their data center. For this, automated monitoring technologies must be used, which periodically test the availability of the respective services. Further, periodic, automated security checks have to be used to avoid the usage of outdated security technologies. If the server is located within a client's private network, the client is responsible for monitoring the availability of the provided services. In case of service interruptions, ESD is responsible for restoring the service.

If CHES is running on ESD's server, the database and all data required to run CHES must be synchronized with a hot standby server that can be activated by technicians in case of disaster. Independent of the server's location (ESD's data center or the client's private network) the database and the applications running on the server must be backed up on a daily basis. The backups need to include all data to allow technicians from ESD to re-install the CHES system. The backup file must be stored at a different location than the server, e.g., a dedicated backup server. This policy also applies to the backup server, i.e., the access to the backup server must be appropriately secured.

2.3.4 Related Standards, Policies and Processes

- Data Privacy Policy (cf. Section 2.2)
- Data Archival Policy (cf. Section 2.4)
- Good Clinical Data Management Practices [1]
- Guidance for Industry, Computerized Systems Used in Clinical Investigations (1999) [5]
- Guidance for Industry, Computerized Systems Used in Clinical Investigations (2007) [6]
- Code of Federal Regulations, Title 21, Part 11, Electronic Records; Electronic Signatures [4]
- Guidance for Industry, Part 11, Electronic Records; Electronic Signatures — Scope and Application [7]
- Guidance for Industry, Electronic Source Data in Clinical Investigations (2013) [9]
- Guidance for Industry, Patient–Reported Outcome Measures: Use in Medical Product Development to Support Labeling Claims (2009) [8]
- IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit [2]

2.3.5 Revision History

- Gerhard Rumpold (2009-04-16): Version 1.0 of the policy.
- Gerhard Rumpold (2013-09-01): Version 2.0 of the policy.
- Jakob Pinggera (2016-05-13): Version 3.0 of the policy.
- Jakob Pinggera (2020-01-21): Version 4.0 of the policy.
- Jakob Pinggera (2020-02-06): Version 5.0 of the policy.
- Jakob Pinggera (2020-08-27): Version 6.0 of the policy.

2.4 Data Archival

After completion of a clinical trial, it has to be ensured that the collected data is archived in a standardized way in order to guarantee their future availability. Further, it has to be guaranteed that no unauthorized access to the data can occur.

2.4.1 Purpose

This policy is intended to regulate the procedure conducted after the completion of a clinical trial. For this, the policy is based on the data storage and data closure guidelines provided in [1].

2.4.2 Scope

This policy is directed to system administrators at ESD, who are responsible for data archival after the completion of a clinical trial. Further, it is of interest for users of CHES as it regulates the availability of the collected data.

2.4.3 Policy

Database closure

Database closure or locking of the a clinical trial's database is essential in order to prevent inadvertent or unauthorized modifications once the data analysis and data reporting have started. While the organizational aspects of closing a database are left to the principal investigator of the clinical trial (cf. [1] on how to define a standard procedure for database closure), ESD strives for providing the best possible support to researchers. As a result, following steps are performed once the principal investigator decides to close the database.

- The access to CHES is revoked for all users unless they are members of the most critical study personnel.
- All parts of the database containing study relevant data, e.g., patient data or PRO data, is put into a read-only state that prevents any modifications to the collected data.
- The point in time when the database is closed is recorded in the system and made available to the principal investigator. In case the database has to be altered, e.g., due to identified errors in the data, all future unlock and lock operations are documented. The principal investigator is responsible for all decisions regarding locking and unlocking of the database.

Data archival performed by ESD

As described in Section 1.2, CHES can be utilized in different scenarios. In case CHES is running on the client's server infrastructure, the client is responsible for data archival. If the data is stored on servers provided by ESD, ESD performs the following procedure.

The installation of CHES remains online for another six months (unless specified otherwise by the client), but access is restricted to the most critical study personnel. After six months, the CHES installation is uninstalled from ESD's servers and the following steps are performed to guarantee the future availability of the data.

- A raw dump of the database is created. This dump also contains the complete audit trail for this instance of CHES.
- All collected data is exported to a human readable data format, e.g., a Comma Separated Values (CSV) file, in order to guarantee access to the data in the extremely unlikely case of not being able to restore the CHES installation.
- The above mentioned data is stored together with all requirements and documentation that has been obtained by ESD from our client (cf. Section 2.1). Additionally, meta-data regarding the utilized version of CHES, the server infrastructure, e.g., operating system or database vendor and version, have to be added. The complete data is encrypted and stored on a machine that cannot be accessed from the Internet.

2.4.4 Related Standards, Policies and Processes

- Data Security Policy (cf. Section 2.3)
- System Implementation Policy (cf. Section 2.1)
- Good Clinical Data Management Practices [1]

2.4.5 Revision History

- Gerhard Rumpold (2009-04-16): Version 1.0 of the policy.
- Gerhard Rumpold (2013-09-01): Version 2.0 of the policy.
- Jakob Pinggera (2016-05-19): Version 3.0 of the policy.

Glossary

AD Active Directory. 5

agile Agile software development might be defined as a set of principles for software development. In agile software development, requirements and the corresponding solutions evolve via collaboration of self–organizing teams. As a consequence, agile software development promotes adaptive planning, early delivery, evolutionary development, continuous improvement, and encourages rapid and flexible change responses. 1, 2, 7, 9

Case Report Form (CRF) Similar to [1], we use the term case report form (CRF) for systems intended to collect clinical data by utilizing, e.g., electronic medical reports, local electronic data capture systems, and central web based systems. 13

CAT computerized adaptive testing. 8

CHES Computer-Based Health Evaluation System. 1–5, 7–11, 13, 14, 17–19, 21–24

CHES.Admin CHES.Administration is the configuration module for CHES. It can only be accessed by users with the appropriate privileges. 3, 4, 18

CHES.Home CHES.Home can be considered the predecessor of CHES.Portal. Similalry, it allows patients to fill out questionnaires from their home. In contrast to CHES.Portal, CHES.Home does not provide any additional information to the patients. 3, 13

CHES.Main CHES.Main is the main application of the system, which is utilized for managing patients and recording patient data. 3, 4, 13, 14, 23

CHES.Nurse CHES.Nurse provides a lightweight interface for tablets that allows for the efficient collection of questionnaires in a clinical setting. CHES.Nurse cannot be used without CHES.Main. 3, 4, 8

CHES.Portal CHES.Portal provides patients with online interface accessible from their home. CHES.Portal provides patients with information specific to their disease and allows them to fill out PRO questionnaires from home without the need to come to the hospital. 3, 4, 8, 13, 23

CHES.Portal-Admin CHES.Portal-Admin is a content management system complementing CHES.Portal. It allows for the customization of CHES.Portal website. 3, 4

CIS clincial information systems. 5

client This document uses the term client to refer to all types of organizations that make use of CHES. In a typical scenario, a client is equivalent to a hospital that runs a CHES installation. 1–3, 7–11, 13, 14, 17–19, 21, 22

CSV Comma Separated Values. 22

CTMS Clinical Trial Management System. 1

eCRF Case ReportForm. 1

eISF Investigator Site File. 1

ESD Evaluation Software Development. 1–3, 5, 7–11, 13, 14, 17–19, 21, 22

eTMF Trial Master File. 1

FTP File Transfer Protocol. 5

HL7 Health Level-7. 5

https Hypertext Transfer Protocol Secure. 18

Kerberos Kerberos (protocol). 5

LDAP Lightweight Directory Access Protocol. 5

PDF Portable Document Format. 5

PRO Patient Reported Outcome. 1, 8, 9, 18, 21, 23

ssh Secure Shell. 18

VPN Virtual Private Network. 10

Bibliography

[1] Society for Clinical Data Management. Good clinical data management practices, 2005.

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI). IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit, 2020.

[3] Chad J. Gwaltney, Alan L. Shields, and Saul Shiffman. Equivalence of electronic and paper-and-pencil administration of patient-reported outcome measures: A meta-analytic review. *Value in Health*, 11(2):322–333, 2008.

[4] U.S. Department of Health an Human Services-Food and Drug Administration (FDA). Code of federal regulations, title 21, part 11, electronic records; electronic signatures, 1997.

[5] U.S. Department of Health an Human Services-Food and Drug Administration (FDA). Guidance for industry, computerized systems used in clinical investigations, 1999.

[6] U.S. Department of Health an Human Services-Food and Drug Administration (FDA). Guidance for industry, computerized systems used in clinical investigations, 2007.

[7] U.S. Department of Health an Human Services-Food and Drug Administration (FDA). Guidance for industry, part 11, electronic records; electronic signatures — scope and application, 2007.

[8] U.S. Department of Health an Human Services-Food and Drug Administration (FDA). Guidance for industry, patient-reported outcome measures: Use in medical product development to support labeling claims, 2009.

[9] U.S. Department of Health an Human Services-Food and Drug Administration (FDA). Guidance for industry, electronic source data in clinical investigations, 2013.

GENERAL TERMS AND CONDITIONS
OF RUMPOLD & HOLZNER OG - EVALUATION SOFTWARE DEVELOPMENT (ESD)
FOR THE SUPPLY OF SERVICES AND THE GRANT OF RIGHTS IN CUSTOM SOFTWARE

SECTION 1
SCOPE

1.1 These General Terms and Conditions (T&C) shall apply to the development, the creation and the purchase as well as the grant of rights in computer programmes, especially in custom software for the computer-based administration and evaluation of health-related data (hereinafter: Software Solution) and shall also apply to related services and independent services used to edit, evaluate and process health-related data (cf. Section 2.6 below) and to highly specialised IT services.

1.2 Any Terms and Conditions of the client which deviate from these T&C or from any amendments and modifications confirmed in writing by ESD are hereby expressly excluded. Any amendment or additional agreement must be confirmed in writing to be effective and shall only apply to the respective case.

1.3 Until ESD issues new T&C, these T&C shall also apply to all future cases, even if those are concluded without any reference to these T&C.

SECTION 2
CONCLUSION OF CONTRACT

2.1 Basis of the business relationship is the respective order which shall define all agreed services (scope of services) and compensations. Unless otherwise noted, offers by ESD are binding for four months at most. Orders are based on the written specifications which shall be prepared by ESD free of charge and shall be based on the documents and information made available. The implementation of the services hereunder shall be called “Project” hereinafter.

2.2 The client has to verify the specifications as to accuracy and completeness and has to provide his/her approval. Any later request for modification or expansion may delay agreed appointments and shall entitle ESD to separately invoice the additional expenses

2.3 ESD warns and explicitly points out that as technology stands today it is impossible to create software programs totally free from defects. ESD, therefore, can only provide a limited guarantee for software products created by ESD (see Section 15).

2.4 In signing this agreement and placing this order the client states that he/she has reviewed the contractual specifications and that the commissioned services as well as the intended scope of services of the Software Solution fulfil his/her requirements. Services which are carried out either before having been specifically defined or without having been defined or having been implemented additionally as well as services which have been marked “variable” in the specifications of services, shall be charged based on the actual time spent.

2.5 Mailshots, brochures and other general product information (e.g. on the ESD website) are not binding unless confirmed in writing by ESD. Any commitments made by ESD employees or agents shall be irrelevant unless confirmed in writing by ESD.

2.6 ESD offers in particular the following services:

2.6.1 development of custom software, particularly software based on “CHES” standard software;

2.6.2 granting of non-exclusive exploitation rights in the Software Solution;

2.6.3 counselling and implementation services, particularly installation and parameterisation of the Software Solution as well as connection of the Software Solution to the interfaces specified by the client;

2.6.4 assistance when implementing the Software Solution (implementation support);

2.6.5 supply a documentation of the Software Solution;

2.6.6 supply of training services;

2.6.7 software maintenance;

2.6.8 database setup, data processing services;

2.6.9 sale of hardware;

2.6.10 other services, especially scientific services.

2.7 It is agreed that each order and the included services shall be regarded as service agreement and not as a contract for services.

SECTION 3
OBJECT OF AGREEMENT

3.1 The Software Solution, which ESD, as licensor, specifically developed, created and handed over to the client upon signing the agreement, is a custom software developed and programmed according to the individual requirements of the client and is based on a specification sheet. In case the custom software is based on the standard software “CHES” developed by ESD, the client, by placing an order acknowledges to be aware of the scope of services included in the “CHES” standard software. Oral statements shall be included in the scope of services only if confirmed in writing by ESD.

3.2 It is agreed that the Software Solution is the exclusive intellectual property of ESD irrespective of the client’s collaboration and irrespective of existing or future laws and jurisdiction. The client’s rights in the Software Solution are exclusively defined according to the respective order.

3.3 Unless otherwise explicitly agreed, the client shall be granted the non-exclusive right in perpetuity to use the Software Solution at the agreed location (non-exclusive exploitation rights) in compliance with these T&C and in compliance with the instruction book provided by ESD only after payment in full of the total amount due (cf. Section 17 below). Unless otherwise expressly agreed in writing, only the client shall be granted this right of exploitation (licence) and shall not be granted to a third party, especially not companies affiliated under company law, e.g. affiliated companies

3.4 Unless otherwise agreed, the Project shall be carried out in two stages. The client shall make the requirements specification available in writing to ESD. These requirements specification shall define the basic requirements of the Software Solution and its implementation and shall also describe the system environment used by the client. During the first stage (cf. Section 4 below) the client shall

3.4.1 analyse the client’s system environment as to its suitability for the Project and

3.4.2 prepare functional specifications, which include the detailed description of the Project and as a technical document it must be suitable to implement the Project. After accepting the functional specifications the second stage starts according to these specifications.

3.5 The purchase of the Software Solution can be combined with the order of software updates. On the client’s request, ESD shall provide updates with costs at dates specified by ESD. The client shall provide necessary hardware and system software upgrades at his/her own expense and responsibility. Technical innovations shall be documented systematically. Updates can be purchased at the respective price communicated by ESD.

3.6 Installation services are included in the order (Section 2) only if this has been expressly agreed and expressly result from the respective specifications. Otherwise, separate charges will be invoiced.

3.7 The agreed fee does not include costs for the use of transmission equipment and lines.

SECTION 4
PLANNING PHASE AND FUNCTIONAL SPECIFICATION

4.1 Prior to development and creation, especially prior to programming and implementation of the Software Solution, the client and ESD shall conduct a planning phase for the implementation of the various Project parts (milestone plan) according to a time pattern in order to define the technical, commercial and chronological modalities in detail.

4.2 Within the scope of the planning phase, ESD may prepare functional specifications which always comprehensively (= conclusively) describe the tasks accepted by ESD, unless otherwise expressly agreed in writing. Such functional specifications by ESD shall be prepared according to best available technology and shall include the following areas:

4.2.1 Goal/non-goals
4.2.2 Technical specifications
4.2.3 Functional specifications
4.2.4 Interface connection
4.2.5 Implementation plan.

4.4 The client is obliged to provide all information ESD requests to evaluate the system environment. After joint consultation, the client and ESD shall define the necessary system environment according to the evaluation in a separate document.

The client shall be responsible for any possible adjustment of the system environment; if ESD has to render services in this respect, a separate agreement shall be required.

4.5 Upon completion of the functional specifications, these shall be accepted and signed jointly. These shall then be part of the specification of services and an integrated part of the order and the agreement

4.6 The planning phase shall verify the intended chronological handling of the Project as specified in the milestone plan and shall define necessary adjustments of the milestone plan mutually and consensually.

SECTION 5
FEE, PRICES AND PAYMENT

5.1 Unless otherwise expressly agreed in writing, the amount of the fee does not include value added tax and is ex ESD’s seat or place of business.

5.2 The client will be separately invoiced for order modifications or additional orders as well as travel expenses, per diems and accommodation. The specific regulations are defined in the specification of services.

5.3 ESD is entitled to a fee for every single service provided. This shall also apply to services not implemented by ESD as intended for reasons ESD is not responsible. All order-related services which are not specifically compensated by an agreed flat-rate fee shall be invoiced separately.

5.4 The prices listed in the specification of services are binding until the date of expiry set forth in the specification of services.

5.5 ESD is entitled at any time to require payments on account for both the agreed fee and cash expenditures. Adequate payments of account for cash expenditures, however, shall be due upon placing of the order.

5.6 ESD is entitled to invoice its services on a monthly basis. ESD is entitled to provide partial delivery and to invoice for partial delivery for orders including several units and program modules.

5.7 Payment shall be made in full within 30 days of the invoice date. If part payments have been agreed and the client defaults on the payment of one instalment, the whole sum shall be payable immediately.

5.8 In case of default, ESD shall be entitled to charge the legally applicable default interest. In case of default of payment within the stipulated time period, ESD reserves the right to charge arrears fees of EUR 40,00 net for each (separate) reminder and for all arising expenses due to claims by third parties (lawyer's fee and costs of collection agency) in accordance with the applicable lawyer's fees and Collection Fee Regulation.

5.9 Compliance with the agreed payment dates constitutes an essential condition for the implementation of delivery or performance of contract by ESD. In case of non-compliance with the agreed payment dates, ESD shall be entitled to stop the current work within one week after written notice and to withdraw from the agreement. All costs involved as well as loss of profits shall be paid by the client.

5.10 In case of failure to comply with the agreed payment dates, or if circumstances adversely affecting the creditworthiness of the client become known, ESD shall be entitled to request advance payments for outstanding supplies and services.

5.11 The client shall obtain the licence granted by ESD only after full payment has been made (cf. Section 3.3 above, Section 17 below).

5.12 Payments with discharging effect can only be made directly to ESD. In case of several unsettled accounts, payments shall be offset with the earliest account. Payments shall always apply first to possible costs, then to the interests and finally to the principal claim.

5.13 The client shall have the right of set-off, only if claims are accepted in writing or are legally established.

Section 6
PROJECT MANAGEMENT AND SERVICES, CLIENT'S DUTY TO CO-OPERATE

6.1 The successful implementation of the Project requires a project organisation corresponding to the size and complexity of the task as well as a coordinated project management of both parties.

6.2 Scope and content of the services provided by ESD shall be defined in the specifications. Unless otherwise specifically agreed, the client shall be solely responsible for providing, accurately investigating and examining the up-to dateness, correctness and completeness of the entire content and data of the Software Solution.

6.3 ESD shall provide its services in close cooperation with the client. ESD and the client shall each nominate a project manager who both shall define the following parameters:

6.3.1 Frequency, duration and group of participants of project meetings;

6.3.2 Level of detail of the project plans and project controlling;

6.3.3 Guidelines to prepare and approve the minutes of the meeting.

6.4 So far as is in his/her power the client shall be responsible to ensure project continuity, i.e. to avoid constant change of staff.

6.5 The client and ESD shall be obliged to immediately inform the other party of circumstances of whatever kind which considerably obstruct the progress of the project, irrespective of whether such circumstances are within one’s own, the other party’s or a third party’s control. In such a case, the project managers shall jointly define adequate measures that come closest to the original project objective.

6.6 If ESD believes that the present project management structure is not accordingly implemented and that the client does not meet, as agreed, the tasks allocated within the scope of the project management, ESD must communicate this immediately. ESD can claim a lack of implementation of the project management structure or possible failures by the client in this context, only if ESD notifies the client of such lacks and failures in writing sufficiently specifying the services to be rendered by the client and setting an appropriate time limit.

6.7 Individual organisational concepts and programmes shall be developed according to type and scope of the binding information, documents and auxiliary material completely provided by the client. This also includes practice-oriented test data and sufficient testing opportunities which shall be provided by the client in due time.

6.8 The client undertakes to ensure that sufficiently qualified staff, facilities, rooms and test data are available at the appointments determined by the project managers at the client’s location. The client provides this cooperation at his/her own costs and expenses.

6.9 ESD shall carry out tests on their staging servers. Live systems can be set up either at ESD on servers provided by the client or at the client’s premises. In case the client authorises ESD to also supply hardware, system software or similar, a separate agreement shall be concluded and a separate specification of services shall be prepared.

6.10 In case the client obtains hardware, system software or similar from third parties, ESD shall upon request assess the basic suitability of these facilities for the proposed objectives. Services such as costs for tests, set-up of the client’s facilities or similar shall be invoiced according to actual time and effort, unless included in the specification of services

6.11 In both cases, the client shall bear the costs and risks for the ongoing operation of the facilities, including technically and organisationally adequate data backup, protection against unauthorised access and virus attacks.

6.12 ESD shall be entitled to submit outlines, especially protocols and written outlines of both general and detailed specifications, to the client for approval. The project managers shall jointly appoint the dates for the documents’ submission and review. In case the approval is delayed due to reasons beyond ESD’s control, ESD shall not be liable for the ensuing scheduling delay. Moreover, ESD shall regard outlines as (partly) approved if a notice of defects is not submitted within two weeks after asking for approval and shall base the next steps of the project on these documents

6.13 Requests for modification or changes in requirements after having completed the specifications and the client’s approval of the preparations may delay the agreed appointments and cause additional expenses

ESD, therefore, shall review such requests for modification as to their impact on quality, costs and dates. The costs for this review shall be invoiced separately. In case the request for modification is feasible, the client shall receive an amended or supplemented offer. The Project shall be continued according to the existing requirements until the order is authorised.

6.14 Services which are provided by ESD at the request of the client and which are beyond the originally agreed scope shall be invoiced separately by ESD.

6.15 ESD shall provide its services within the normal hours of work. In case services are provided outside the normal hours of work and at the request of the client, the additional costs shall be invoiced separately. The specific regulations are defined in the specification of services.

6.16 The client shall be separately invoiced for travel expenses, per diems and accommodation. The specific regulations are defined in the specification of services.

SECTION 7
ACCEPTANCE OF SERVICES RENDERED

7.1 Customised Software Solutions and program adjustments need to be accepted by the client no later than 14 days after the delivery by ESD. The project managers shall determine the separate parts and the scheduled dates; the client shall approve the acceptance in a record (review of the services' correctness and completeness according to the order using test data made available by the client). If the client does not specifically accept the program within 10 days, the supplied Software Solution shall be considered accepted as of the last day of the 10-day period. The Software Solution, however, shall be considered accepted as soon as the Software Solution is used in live operation by the client.

7.2 The functional test shall be considered successful, if the Software Solution meets the contractual requirements in all essential points. Possible defects – deviations from the written specification of services – are to be reported to ESD sufficiently documented in writing by the client. ESD shall make efforts to correct the defects as quickly as possible. In case serious defects have been reported in writing, i.e., if real-time operations have not commenced or cannot be continued, a renewed acceptance of the work is required following the correction of the defect.

SECTION 8
REMOTE MAINTENANCE, MAINTENANCE AND SUPPORT

8.1 To ensure prompt support by ESD in case of warranty or in case the client needs other kind of assistance, a remote maintenance access may be installed. All costs (for hardware, software, telephone lines etc.) thereby incurred at the premises shall be borne by the respective party hereto. The project managers shall jointly decide on technical solution and relevant safety aspects.

8.2 The client shall be at liberty to confine remote maintenance access, e.g. to certain times of the day, certain ESD employees or to other criteria.

8.3 In case ESD suffers disadvantage or additional expenses due to non-availability of the remote maintenance access for which the client is responsible, ESD shall invoice the additional expenses separately. ESD shall not be liable for any damages caused by non-availability of the remote maintenance access.

8.4 After the start of live operation further support and software maintenance may be offered. The project managers shall jointly decide on the exact date for the transfer in the support as well as on the transfer details. A separate software maintenance agreement on software maintenance and the scope of services to be rendered by ESD in this context shall be concluded.

8.5 ESD shall perform maintenance to correct faults which occur while using the Software Solution and/or become apparent in the respective application documentation. Classification of faults as well as involved urgency to correct the faults shall be determined according to the respective ESD priorities list. A fault occurs, if the programme does not meet its functions specified in the specifications list, provides wrong results, interrupts its run uncontrollably or does not operate appropriately, so that the program use is prevented or affected. Maintenance shall also include one-time training of the client’s staff on scope and type of the works performed.

8.6 Fault correction shall include localising the cause of defect, diagnostic inspection and correction of fault or, if these measures are not possible at reasonable costs, establishing the operational availability by workaround.

8.7 Other defects are only imperfections of the Software Solution which do not impair its function. Other defects are principally not included in the maintenance. Such defects shall be corrected by ESD only if justified at reasonable costs. Latter shall not apply if the defect can only be corrected by reprogramming essential parts of the program in question.

SECTION 9
DEADLINES AND RIGHT OF WITHDRAWAL

9.1 ESD shall aim to meet deadlines (completion) as agreed.

9.2 Target completion dates can be met only if the client provides all required works, dates and documents in full, especially the specifications list and preparations accepted by the client, on the dates specified by ESD and the client fulfils his/her obligation to cooperate to the extent required.

9.3 Delays in delivery and additional expenses resulting from incorrect, incomplete, or subsequently changed data, information and supporting documentation provided to ESD, shall not be the responsibility of ESD and ESD is not to be held responsible for the default of delivery. Additional expenses arising shall be borne by the client.

9.4 Unexpected, unpredictable events such as Force Majeure, labour dispute, natural disaster shall allow both parties hereto to agree on new deadlines.

9.5 In the event of missing the agreed deadline through fault of ESD, the client is entitled to set an extension of delivery time of at least four weeks, at the end of which he/she may withdraw from the order in writing by certified mail, if the agreed services have not essentially been rendered during the set extension of time. However, it is not possible to withdraw from already rendered partial deliveries and services.

SECTION 10
RIGHTS IN THE SOFTWARE SOLUTION

10.1 The Software Solution, which ESD, as licensor, provided to the client, is a custom software developed and programmed by ESD based on the standard software CHES and according to the individual requirements of the client (and according to the specifications list). The client’s cooperation in the development of the Software Solution shall not confer any rights beyond those exploitation rights stated herein.

10.2 The client's rights in the Software Solution are solely determined by the respective order (non-exclusive exploitation rights).

10.3 In case the Software Solution includes interfaces to external computer programs, especially open source software, these shall not be part of the Software Solution. ESD does not accept any liability for defects of third party's software connected (see also Section 15.8). The client accepts the applicable license terms of such involved software parts, especially open source software licenses, if any (e.g. Black Duck Software, GNU General Public License (GPL v2 and v3), Massachusetts Institute of Technology License (MIT), Apache License 2.0, Berkeley Software Distribution License 2.0 (BSD), GNU Lesser General Public License (LGPL v2 and v3), Artistic License, Mozilla Public License (MPL), Eclipse License (EPL) or Code Project Open License).

SECTION 11
RIGHT OF REPRODUCTION AND ACCESS PROTECTION PURSUANT TO NON-EXCLUSIVE EXPLOITATION RIGHTS

11.1 If the non-exclusive exploitation right is granted, the client may reproduce the supplied Software Solution insofar as the respective reproduction is required to use the program and all license regulations are observed. Required copies comprise the installation of the software from the original data medium to the mass storage device of the hardware used as well as the download of the Software Solution to the working memory. Loading the supplied Software Solution to a network or other multi-function data processing systems is subject to Section 12.

11.2 Furthermore, the client may generate a copy as backup. However, only a single backup copy may be generated and stored. This backup copy is to be marked as a backup copy of the granted Software Solution.

11.3 The client shall implement precautions to prevent any unauthorised access by third parties to the Software Solution and the documentation. The original data media supplied as well as the backups shall be stored at a site protected against unauthorised access by third parties. The employees of the client shall be strongly advised to observe these terms of contract and the provisions of the copyright law.

11.4 The client shall not produce other copies which also include the output of the program code on a printer as well as photocopies of the user's manual. Manuals possibly needed for employees have to be obtained exclusively from ESD.

SECTION 12
MULTIPLE USE AND USE IN A NETWORK ENVIRONMENT PURSUANT TO NON-EXCLUSIVE EXPLOITATION RIGHTS

12.1 The client is entitled to use the Software Solution on any hardware at his/her disposal. The hardware used, however, must be suitable for the use of the Software Solution. In the event, however, that the client changes the hardware, the Software Solution has to be deleted from the hardware used so far.

12.2 The installation of the granted Software Solution in a network or another multi-user system and the concurrent loading, saving or use in more than one independent computer hardware shall be allowed only in compliance with the respectively granted software licenses.

SECTION 13
DECOMPILATION AND PROGRAM MODIFICATION

13.1 The translation of the program code granted to the client into its code form (decompilation) and other methods of reinterpreting the various production steps of the Software Solution shall be allowed

13.1.1 if this is indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs;

13.1.2 if these acts to achieve interoperability are exclusively performed by ESD (see Section 13.4);

13.1.3 if the information necessary to achieve interoperability has not yet been published or been readily available and

13.1.4 if these acts are confined to the parts of the Software Solution which are necessary to achieve interoperability.

13.2 The provisions of Section 13.1 shall not permit the information obtained through its application to be used for goals other than to achieve the interoperability of the independently created computer program. This information shall not be given to others, except when necessary for the interoperability of the independently created computer program. This information shall not to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright of ESD.

13.3 Removing the copy protection or any similar protection mechanism is only permitted if this protection mechanism interferes with or prevents error-free use of the program (see Section 16.2 for the approach to be followed). The client must prove that the use is impaired or hindered by such a protection mechanism. The provisions of Section 17 of the present T&C (reservation of title) have to be taken into account in this context.

13.4 All acts listed above shall only be allowed for commercial purposes. Moreover, they shall not be given to others except when ESD refuses to perform the requested program modification upon a reasonable fee. The client shall allow ESD sufficient time for review and acceptance of such an order and shall provide the name of the third party.

13.5 Copyright notices, serial numbers and other marks used to identify the program must on no account be removed or modified.

Section 14
Prohibition Of Resale And Sub-Lease Pursuant To Non-Exclusive Exploitation Rights

If the client has been granted a non-exclusive exploitation right and not an exclusive exploitation right (cf. Section 3.3 above), the client shall not be permitted to sell or transfer the Software Solution, including the user manual and other accompanying materials to third parties free or against payment, especially not to give away, lease or lend the Software Solution to third parties. The use of the Software Solution by the client’s employees within his/her scope of business shall not be affected thereby.

Section 15
Warranty And Damages

15.1 The warranty period shall be twelve months from the acceptance date (cf. Section 7 above). Any claims for defects of the supplied Software Solution, including user’s manuals and other documents, asserted within this period, shall be eliminated by ESD within a reasonable period of time following the receipt of the letter of complaint in due form. ESD shall at its discretion provide either rectification or replacement. ESD shall start the work to remedy defects within 36 hours following the receipt of the letter of complaint. In the event that an inspection shows that there is no defect (for which ESD is responsible), ESD is entitled to claim reimbursement of expenses according to ESD's standard hourly rates plus reasonable expenses. ESD shall not be held liable for defects identified after the expiration of the warranty period (e.g. bugs, security holes). The client shall submit possible warranty claims in writing within two weeks after the defect first became apparent. Such a letter of complaint shall include a detailed description of the defects. A sufficient documentation of the defects shall be submitted four weeks after becoming apparent. If the complaint is justified and submitted in due time, the client shall be entitled only to improvements of the service (rectification of defects or replacement delivery). The client shall be entitled to reduction in price and to rescind the contract only if ESD's attempts to remedy defects fail even after three months, or in case of more complex defects within an appropriately longer period of time. The presumption of defectiveness pursuant to Section 924 ABGB (Austrian Civil Code) shall not apply.

15.2 ESD shall not be liable for any damages, except where these violations of contract arise from wilful act or gross negligence on the part of ESD. The client's right to warranty shall not be affected in compliance with these T&C. However, claims by the client for consequential loss and damage caused by defect, especially loss of profit and claims by third parties shall be excluded.

15.3 After a possibly agreed training, the client has to ensure that instructions for use are known and observed. ESD shall not be held liable if the client or a third party modifies the Software Solution on his/her own authority. ESD shall invoice expenses for support, diagnostic inspection and for defect rectification for which the client is responsible, as well as for other corrections, amendments and modifications. This shall also apply to the correction of defects caused by program modifications, amendments or other interventions which were performed by the client or a third party.

15.4 Moreover, ESD shall not be held liable for defects caused by inappropriate use, modified hardware, components of the systems software, interfaces and parameters or caused by the use of unsuitable means of organisation and data media and similar or caused by damages in transit. ESD shall not assume any liability whatsoever for the loss of data.

15.5 ESD does not assume any liability for documents made available by the client. The client, however, shall be liable for ensuring that none of the documents made available by him/her for processing violate the rights of third parties, that these documents are allowed to be used for the purpose for which they are intended to be used and do not violate any existing law. If the client subsequently becomes aware that the documents submitted are unsuitable for use, the client shall notify ESD immediately and shall reimburse ESD for possible expenses thereby incurred.

15.6 ESD shall at all times be entitled to reject or remove materials, documents and the like provided by the client which violate existing law or where there are reasonable grounds for suspecting such a violation. This shall not give rise to any claims by the client.

15.7 Unless a legal review has expressly been included in the contract, the client shall solely be responsible for ensuring compliance with all legal provisions, especially provisions of copyright, patent law, medical devices act, data protection act, competition law or trademark law, when implementing measures (cf. Section 18.8 below). Therefore, ESD shall not be held liable in any case. The client declares to hold ESD harmless from third party claims based on such violations.

15.8 ESD shall not assume liability for third-party libraries dynamically linked via the Software Solution and which are used by the client. Moreover, ESD shall not assume liability for the correct executability of the Software Solution's modules with other versions (e.g. software updates) of third-party computer programs. ESD shall not assume any liability whatsoever for third-party computer programs linked to the Software Solution.

15.9 ESD's liability for both personal and material damages shall be limited to damages which are to be expected in the course of a software transfer, and shall in any case be limited to the purchase price. Insofar as ESD is liable for damages, notwithstanding Section 15 herein, ESD shall be entitled to be discharged from all liabilities by assigning to the client all claims held by ESD against the liability insurance

SECTION 16
DUTY TO INFORM PURSUANT TO NON-EXCLUSIVE EXPLOITATION RIGHTS

16.1 If the Software Solution has especially been adjusted to the client's hardware, the client shall be obliged to notify ESD in writing of any change in hardware. The same applies in the event that the client wants to use the Software Solution concerned within a network.

16.2 The client is obliged to notify ESD in writing and in advance of decompilation or any other change in program. The client has to provide a detailed description of the conditions precedent (cf. Section 13) to such an approved program modification. This duty to inform includes a detailed presentation of these conditions, such as symptoms of the occurred defect, assumed reasons for the defect and detailed description of the program modification performed. It is prohibited to perform such measures without prior information. In compliance with the first sentence of Section 13.3, it is, however, prohibited to remove a copy protection or any other similar protection routine from the program code

SECTION 17
RETENTION OF TITLE AND RESERVATION OF USE

17.1 ESD shall retain title and the non-exclusive exploitation right to the Software Solution supplied to the client until full payment of all amounts due have been made. Only limited licenses shall be granted until full payment has been received. The client shall obtain an extension of time for payment from ESD preceding the expiration of the time limit. The expiry of a limited license due to payment not made on time shall not affect the client's obligation to full payment.

17.2 If the client is responsible for arrears or materially breaches duties of diligence and care, ESD's assertion of retention of title and reservation of use shall not be considered a withdrawal from contract unless expressly notified by ESD.

SECTION 18
RESULTS, REGISTRATION OF PROPERTY RIGHTS, THIRD-PARTY PROPERTY RIGHTS

18.1 Results as defined by this agreement are inventions subject to property rights, qualified know-how pursuant to the Commission Regulation (EC) No 772/2004 of

7 April 2004 as well as know-how not subject to property rights. Joint results are results achieved by both parties hereto, with each party providing a creative share.

18.2 If ESD or employees of ESD develop inventions subject to property rights in the course of the order, ESD shall exclusively be entitled to these inventions. The same shall apply to rights to jointly developed content.

18.3 If the joint results are employee inventions (joint invention), the parties hereto undertake to assert, in time, all rights to the inventions against their employees. Internally, the rights to the invention shall be divided between the employees proportionally to the respective contribution in the invention.

18.4 In case existing property rights of ESD are used, or such rights arise in order to implement the contract, the client shall be granted the non-exclusive and free exploitation right for the contractual purpose.

18.5 Concepts, expertise etc. by ESD are copyrighted. ESD shall solely be entitled to the copyright in these works. Unless expressly agreed otherwise, ESD only grants non-exclusive exploitation rights, but not exclusive exploitation rights. Non-exclusive exploitation rights to be granted to the client need to be approved in writing by ESD, unless it is implied in the scope of the contract.

Unless agreed otherwise, the non-exclusive exploitation right in copyrighted works of ESD granted to the client shall be confined to the application range specified herein.

18.7 The client undertakes to examine property rights or have property rights related to the contract examined, especially third-party property rights. In case third-party property rights are needed to successfully implement the works, the client shall immediately notify ESD in writing. The client shall decide whether a licence is requested or the works are continued in such a way as not to violate any third-party property rights.

18.8 The client undertakes to examine the legitimacy of all measures related to the Software Solution or have the legitimacy of all measures related to the Software Solution examined, especially as to data protection and copyright.

SECTION 19
WRITTEN FORM

Any amendments, modifications or specifications, especially warranties and agreements, to this contract must be in writing to be legally applicable. In case they are explained by representatives or auxiliary persons of ESD, they shall only be valid if approved in writing by ESD. E-mails also comply with the written form requirement.

SECTION 20
DATA PRIVACY, CONFIDENTIALITY, REFERENCE LIST

20.1 ESD shall be responsible for ensuring compliance with Section 15 of the Data Protection Act 2000 on the part of its employees. Both parties agree to keep the content of the contractual arrangements and all internal information and data of the other party that a party receives in connection with the cooperation between the parties confidential and not to disclose them to third parties.

20.2 Any publication of work-results by a party to the agreement that goes beyond the mere fact of the placement of an order and the related basic information (company name and address, general list of application areas, approximate number of users and similar) requires the explicit approval of the other party.

20.3 This contractual confidentiality does not apply to court hearings or to professional representatives of the parties who are sworn to secrecy, especially at court actions or settlements out of court (e.g. fee lawsuits) insofar as it is necessary to protect the rights of ESD.

20.4 Notwithstanding this duty of confidentiality, until revoked in writing ESD shall be entitled to include the client and possible descriptions of rendered services in the reference list, and to use this information for any fair advertising and presentation service, especially in the internet.

Section 21
FINAL PROVISION

21.1 Place of performance and jurisdiction is A-6020 Innsbruck. This agreement shall be subject and construed according to Austrian Law to the exclusion of the UN

Sales Convention on Contracts for the International Sale of Goods as well as to the exclusion of the conflict of laws and ROM I. In the event that any industrial property right is violated in a foreign country, the more favourable law for ESD applies.

21.2 The client shall not be entitled to offset counter-claims against claims by ESD or to withhold payment referring to defects. The client shall only be entitled to offset claims against legally established claims by ESD or to assert a lien.

21.3 The invalidity or unenforceability of any provision of this T&C or agreements amended by such provisions shall not affect the validity or enforceability of this Agreement. The parties hereto agree to replace any invalid provision with a provision that is valid and comes closest to the original intention of the invalid provision.

21.4 Any amendments, modifications or side-agreements to this T&C as well as any warranty must be in writing to be legally applicable. This shall also apply to agreements to change this formal requirement.

***