CHIC End User Agreement

(Version 1.0, March 2014)

between

the Center for Data Protection ("CDP")

Rempart de la Vierge, 5, Namur, Belgium 5000

hereinafter "CDP"

and

Foundation for Research and Technology – Hellas (FORTH)
("CHIC end user")

N. Plastira 100, Vassilika Vouton, 70013 Heraklion, Greece
(address and country of establishment)

Individually referred to as a "Party" or collectively referred to as the "Parties".

Preamble

The Computational Horizons In Cancer (CHIC) project is a EU-financed FP7 project that aims to create an infrastructure for the development of a number of integrative multiscale cancer models and hypermodel oncosimulators. These will be clinically adapted and partly validated, a process which will involve sharing of clinical and genomic data of patients within the project. At the same time each of the partners recognises as a priority the imperative need to respect the fundamental interests and rights of patients, including the need to preserve the security and privacy of personal data involved in the project.

Therefore the Infrastructure of CHIC is embedded in the CHIC Data Protection Framework, which guarantees compliance with current European data protection legislation, primarily by de facto anonymising the patient data. Due to the diverse participation of researchers in the project, it is of high importance to process patient data in compliance with all applicable laws and regulations, including without limitation, privacy and medical secrecy laws applicable to the activities of the parties.

To fulfil the objectives of the project, the data will be de-identified, using secure state of the art pseudonymisation/de-identification tool (eg, CATS), on-site by the respective data providers to the project, before it is subject to a second round of encryption by the Center for Data Protection (CDP) and transferred to secure, access-controlled data repositories within the CHIC infrastructure. The CDP will transfer the original (data provider) code to an independent trusted third party, and the latter alone will retain the pseudonymisation key (cross table) needed to link the double-encrypted CHIC data set to the initial deidentified data sets provided by the data providers. This shall enable the project's partners to exchange patient data as end users, within a closed community, in which each of the partners is contractually bound to implement all necessary technical and organisational safeguards to protect the data. Pursuant to the CHIC description of work, the CDP operates as the central data controller for the CHIC infrastructure.

This agreement is needed to state the conditions and obligations under which the CHIC end-users (scientific and technical partners, including modellers and tool developers) will process data within the said infrastructure.

Clause 1: Definitions

For the purposes of this agreement, the terms used in these clauses shall have the same meaning as attributed to them in the General Framework Terms in Annex A to this agreement.

Clause 2: Scope and responsibility

1. This Agreement sets out the terms and conditions for the CHIC technical partners, including modellers and component developers working in the project (end users) to access, use, and share patient data within the CHIC infrastructure.

2. The CDP is responsible as data controller for the management of the CHIC infrastructure, while the CHIC end user is responsible for the data it accesses and uses from the infrastructure within its own organisation.

Clause 3: Obligations of the CDP

The **CDP** warrants and undertakes:

1. to grant to the end user a non-exclusive right to access and use the data in the CHIC data infrastructure (hereinafter the CHIC data) for the purposes of the end user's work within the CHIC project, subject to the provisions of this agreement;

2. that it is entitled to grant access to the CHIC data to the end user as aforesaid;

3. to put in place procedures to ensure that prior to transfer to the CHIC infrastructure, CHIC data are collected and processed in accordance with the laws applicable to the data provider, including by entering into the 'CHIC Data Provider Agreement' with relevant data providers;

4. to have in place appropriate technical and organisational measures to protect patient data within the CHIC infrastructure against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, including by entering the 'CHIC Trusted Third Party Agreement' with the CHIC TTP.

Clause 4: Obligations of the CHIC end user

The **CHIC end user** warrants and undertakes:

1. to process the CHIC data in compliance with applicable data protection regulation and the terms of this agreement; and where it cannot provide such compliance for whatever reasons, it agrees to inform promptly the CDP of its inability to comply, in which case the CDP is entitled to suspend access to the data and/or terminate the contract;

2. to process the CHIC data only for the purposes of its work within the CHIC project;

3. that it has implemented and follows appropriate technical and organisational security measures to protect the CHIC data against misuse and loss (including without limitation the measures stated in Annex B to this agreement), in accordance with the requirements of relevant provisions of European data protection law, and in particular Article 17 of the Data Protection Directive 95/46/EC or any subsequent provision in an EU instrument that may re-enact or replace the same;

4. that it will ensure that where CHIC data is stored within its own organisation, such data is technically and organisationally separated from other data;

5. that it will retain the CHIC data within a secure database or network system at such standard as would be reasonably expected for the storage of sensitive/confidential data;

6. that it shall not attempt to identify any patient from the CHIC data either by external matching of the data or by any other means;

7. that it shall not disclose or publish the CHIC data to any third party, which for the avoidance of doubt includes any of its subcontractors or party with which it has an equivalent arrangement, without seeking and obtaining the specific written authorization of the CDP;

8. that in the event of inadvertently identifying any patient, it will notify the CDP immediately setting out (in reasonable detail) the circumstances by which this occurred. In such a case it further undertakes not to make any use of the identifying information for any purposes and to take all necessary steps to protect the interests of the patient including so far as possible restoring the de-identified status of the patient;

9. to ensure that each of its employees who has contact with the CHIC data is made aware of, and will be bound by, the terms of this Agreement, and such an employee will complete Annex C to this Agreement;

10. to inform the CDP immediately, should the CHIC data, while in the hands of the end user be threatened with seizure or confiscation through bankruptcy or settlement proceedings, or through any other circumstances including the actions of a third party.

11. that if it becomes aware that it is necessary or desirable, in the exceptional circumstances identified Annex A to this agreement, for the CHIC data to be re-linked to the data subject it shall contact the CDP only, so that the latter can initiate the re-identification process with the help of the Trusted Third Party that holds the key to link the de-identified data sets in respect of the subject concerned;

12. to deal promptly and properly with all inquiries from the CDP relating to its data processing and data security measures;

13. that upon reasonable request by the CDP, it will submit its data processing facilities, data files and documentation needed for reviewing, auditing and/or certifying by the CDP (or any independent or impartial inspection agents or auditors, selected by the CDP and not reasonably objected to by the CHIC end user) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The same obligations apply in case a supervisory authority demands auditing;

14. to provide the CDP with contact details of the person responsible for data protection in its organisation;

Clause 5: Cooperation with supervisory authorities

1. The CDP agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable regulation.

2. The parties agree that the supervisory authority has the right to conduct an audit of the CHIC end user which has the same scope and is subject to the same conditions as would apply to an audit of the CDP under the applicable regulation.

Clause 6: Liability and indemnity

.1. Each party shall be liable to the other party for damages it causes by any breach of these clauses. The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred. Indemnification is contingent upon:

(a) the parties promptly notifying each other of a claim; and
(b) each party is given the possibility to cooperate in the defence and settlement of the claim.

2. The parties agree that each party shall be liable for patient's damages it caused by any negligent violation of data protection legislation or any analogous provisions of national or international law.

Clause 7: Penalty

1. The parties agree that subject to the exception in clause 7.3 below, a party in wilful or negligent breach of clause 3 or 4 of this agreement shall pay a penalty of 10.000 (ten thousand) EUR. The enforcement of this clause shall be subject to the finding of wilfulness or negligence by the court under Clause 9 below.
2. The penalty shall be paid to the CHIC Consortium and can be used for specific project purposes which will be determined by the Consortium. A user account approved by the whole CHIC Consortium will be supplied for this purpose.
3. In the event that the breach or series of breaches does not lead to the identification of any data subject, then provided that the party in breach timeously corrects the breach in accordance with the terms of clause 8.2 below, it shall escape the liability set out in this clause.
4. The above provision shall be without prejudice to the parties' right to terminate the contract, to seek compensation for damages or to enforce any claims under this agreement.

Clause 8: Termination and obligations of the parties after the termination

1. This agreement will terminate, if not otherwise superseded or amended by new provisions extending it, at the latest by 31st March 2017.
2. In case of breach of clauses 3 or 4 by one of the parties, the other party is entitled to give written notice requiring the party in breach to be repair the breach within 72 hours, after which time if the breach remains outstanding it may terminate this agreement.
3. Without prejudice to the foregoing provisions, any party may terminate this agreement for good cause, giving the reason for such termination.
4. Each party shall inform the other party by prior written notice in case of termination of the agreement.
5. The parties agree that on the termination of the provision of data processing services, the CHIC end user shall, at the choice of the CDP, return all the CHIC data and the copies thereof to the CDP or shall destroy all the data and certify to the CDP that it has done so, unless legislation imposed upon the CHIC end user prevents it from returning or destroying all or part of the data transferred. In all cases, the CHIC end user warrants that it will continue to guarantee the confidentiality of the data and will no longer actively process the data.

Clause 9: Governing law and Jurisdiction, miscellaneous

1. This agreement shall be governed by Belgian Law. The courts of Brussels/Belgium shall have exclusive jurisdiction. This shall also apply to disputes on the validity of this clause.

2. Changes and amendments to this agreement shall require written agreement signed by the parties and an explicit statement that they represent a change or amendment to these conditions. The same applies to the waiving of this formal requirement.

3. If any provision of this agreement shall be entirely or partly invalid or unenforceable, this shall not affect the validity and enforceability of any other provision. An invalid or unenforceable provision shall be regarded as replaced by such a valid and enforceable provision that as closely as possible reflects the privacy/security and/or economic purpose that the parties hereto had purposed with the invalid or unenforceable provision.

4. Each person signing below and each party on whose behalf such person executes this agreement warrants that he/she, as the case may be, has the authority and the legal capacity to enter into this contractual agreement and perform the obligation herein.

5. This agreement will enter into force on the effective date, i.e. the date of the last binding signature to this agreement.

Made in two signed copies, each party having received its own signed copy.

(Place, Date) (Signature of Nikolaus Forgó (president of the CDP)

5|8|2014

(Place, Date)

Costas Fotakis

(Signature [CHIC end user])

Annex:

A. General Framework Terms - version 1.0 (March 2014)
B. Technical and organisational measures
C. Access authentication form

Annex A

GENERAL FRAMEWORK TERMS

(Version 1.0, March 2014)

The project CHIC (Computational Horizons In Cancer) in this present document, aims at creating and developing models and hypermodels for use in the diagnosis and treatment of cancer. The CHIC project will initially proceed by using data on Wilms tumor, glioblastoma multiforme (GBM), prostate cancer, and non small cell lung cancer (NSCLC), but it is projected to involve further cancer types in the future. The final purpose of such scientific research is to improve cure and management of future cancer patients.

Therefore data repositories will be set up within the CHIC infrastructure to enable the project's partners to share patient data. These repositories will contain patient data transferred to the CHIC infrastructure by the CHIC data providers (participating hospitals/investigators), based on the patients' informed consent to use their data for research within CHIC and/or the approval of the relevant data provider's responsible ethical board or committee.

The patient data remain under the control of the respective hospital/investigator (data provider) where the data are collected until the data have been transferred to the CHIC infrastructure. Prior to transfer the data provider is thus obliged to ensure the confidentiality and protection of the data. These obligations are defined by the contractual agreements concluded with the CDP. After transfer the CDP will be responsible for the security of data processing within the CHIC project.

All data transferred to the CHIC infrastructure will be initially deidentified on-site by using a state of the art de-identification tool such as CATS by the data provider concerned; it will then be subject to a second round of encryption by the CDP using dedicated state of the art encryption software, in which the initial data provider's pseudonym is replaced by a second pseudonym. The pseudonymisation key (cross table) needed to relink the double-pseudonymised data set to the initial pseudonymised set will be transferred from the CDP to the CHIC Trusted Third Party (TTP). The CHIC TTP's independence from the CDP, the data providers and end users will be guaranteed. That means that neither the CDP nor the end user using the data will be unable to re-establish a link to the patient to whom the data relates. In addition contracts are concluded between the partners providing data to, and using data within CHIC and the CDP guaranteeing that patient data are not transferred to any party outside the project and no matching of data set takes place in order to identify the patients concerned. In interaction with strong technical and organisational security measures, patient data in CHIC is to be seen as de-facto anonymous. Further, the CDP controls the enforcement of these contractual agreements. It thus serves as a central data protection authority for the CHIC framework.

At the same time, the key held by the CHIC TTP preserves the possibility in exceptional circumstances of re-identifying a given patient, in particular in the event that a new treatment for him/her is developed. This can occur only with the help of the CHIC TTP and with permission of the CDP, and enables physicians at the data provider institution alone (where the patient concerned is treated) to link the data to the original patient where the patient has expressed their wish for this to occur in their own interests. For the avoidance of doubt, insofar as project-goals, such as the need to test or validate the performance of hypermodels later in the project, make it necessary to re-link data in the CHIC infrastructure to real patients, such re-linkage shall not be permitted without the further specific consent of the patients concerned and/or the obtaining of appropriate ethics body approval.

The CHIC data will be stored for a length no longer than the CHIC project. During the whole term of storage it will always be provided that the data remain de-facto anonymous for the CHIC end users. For a longer storage of patient data the explicit informed consent of the patient or ethics approval will be required. The users (researchers) are not allowed to publish the data or to transmit or disclose data received via CHIC to any third person outside of CHIC.

These General Framework Terms are applicable to the CDP (as a legal person), the CHIC TTP, the CHIC data providers and the CHIC end users.

Explanatory Glossary (forming part of the General Framework Terms):

Anonymous data / Rendering anonymous

Rendering data anonymous means to modify personal data in a way that the information concerning personal or material circumstances can no longer be identified, or it is only possible with a disproportionate amount of time, expense and labour to attribute the data to an identified individual. Data that have been anonymised are no longer "personal data" in the legal sense. It will be an aim to have as much anonymised data within CHIC as possible and reasonable. With the technical and organisation measures taken to secure the data, including the present contractual agreement as well as the CHIC End User Agreement, the data processed within the CHIC infrastructure shall be regarded as (de facto) anonymous data only.

Center for Data Protection (CDP)

The CDP shall mean the central data protection authority of the CHIC infrastructure, which agrees to receive from the healthcare organisations/hospitals (data providers) data intended for processing in accordance with the terms of the Data Provider Agreement. The CDP guarantees privacy within the CHIC infrastructure and repositories.

CHIC data

CHIC data means patient data provided in securely deidentified form by the CHIC data provider partners and, following a second round of encryption by the CDP, transferred to the CHIC infrastructure and repositories for access by the CHIC end users, subject to contractual duties of care, for use in accordance with the purposes of the project.

Confidentiality duty

Persons engaged in data processing within the CHIC project shall not, without authorisation, collect or process personal data, nor publish or disclose such data to any third party. On taking up their duties such persons shall be required to give an undertaking to maintain confidentiality, as set out in Annex C of the End User Agreement. This undertaking shall continue to be valid after termination of their activity. Any person acting under the authority of the CDP who has access to CHIC data must not process them except on instructions from the controller, unless he/she is required to do so by law.

Consent

Informed consent means any express indication of data subject's wishes, expressing his/her agreement to data relating to him/her being processed, provided that he/she has sufficient information about the purposes of the processing, the data or categories of data concerned, the recipient of the data, and the name and address of the controller and of his/her legal representative, if any. The consent must be freely given and specific, and may be withdrawn by the subject at any time. If the subject is incapable of a free decision or domestic laws do not permit the subject to act on his/her own behalf, consent is required of the person recognised as legally entitled to act in the interest of the data subject or of an authority or any person or body provided for by law (legal representative).

Data controller

The data controller/controller is, according to the Data Protection Directive 95/46/EC, the natural or legal person who alone, or jointly with others, determines the purposes and means of the processing of personal data. The data controller is liable for the legality of the processing and the fulfilment of the obligations towards the national data protection authority and the patients. The hospitals/investigators participating in the CHIC project (data providers) are data controllers with regard to the collection of Patient Data and their transmission to CHIC, whereas CDP is the data controller with regard to the data stored in the CHIC infrastructure. Finally the CHIC end-users are in the position of data controllers with the obligation to ensure full confidentiality and security of the data they receive from the CHIC infrastructure and repositories.

Data processor

Data processor shall mean a natural or legal person, public authority, agency or any other body which processes patient data on behalf of the controller, such controller being liable for the legality of the processing and the fulfilment of the obligations towards the national data protection authority and the patients.

Data subject

The data subject is the subject of personal data, meaning an identified or identifiable person the data refers to. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. As a rule the patient, whose data are collected and processed for CHIC will be the data subject, when his/her personal data are processed.

Disclosing

Disclosure is a processing operation in which patient data are provided by a controller to a third party. The data controller must only disclose data to third parties if permitted by law or by the data subject´s consent. In CHIC, data are only shared among CHIC end users who have each signed a special agreement that forbids any disclosure of data received via CHIC to any third party.

Hospital

Hospitals are health institutions where patients are treated and their personal data are collected for the purpose of the CHIC project.

Investigator

The legal or natural person who gathers and manages the patient's data from the hospitals, laboratories etc. and maintains and controls the trial/study database.

Legal representative of the patient ("legal representative"):

The legal representative(s) of the patient is/are the person(s) who has/have the power by law or legal decision to decide for a minor patient (or equivalent status such as mentally disabled patients).

Necessary processing

When deciding which data will be collected and further processed, the controller must limit these data to the extent necessary to achieve the purpose of processing. This means that personal data will only be processed when it is necessary for the project.

Patient:

Patient means the person treated in a hospital. Certain data collected in the hospitals will upon the patient´s consent and/or the obtaining of appropriate ethics body approval be transferred to the CHIC infrastructure where they will be used for the purposes of scientific research in (de facto) anonymous form.

Personal data

Personal data means any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. Therefore a set of data collected under a certain number or sign "patient xxx", "tissue YYY" can be personal data, if the patient concerned can still be identified by other means than his/her name.

Physician

The physician is the natural person who is in charge of the patient's treatment.

Publish

The controller and the processors will refrain from publishing personal data or otherwise making them public, unless specific consent from the patient concerned is obtained.

Purpose

The purposes for processing of personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. The purposes must be specified, explicit and legitimate. Personal data must not be further processed in a way incompatible with those purposes. The purpose for the collection, transfer and use of the data within CHIC is to create cancer models and hypermodels in accordance with the objectives of the project.

Secure Deidentification

To securely deidentify a data set means to employ a state of the art deidentification tool, which replaces the patient's name and other identifying characteristics with a coded label and performs such further appropriate operations (eg, suppressing and/or perturbing other dataset values) in order to preclude reidentification of the patient or to render such reidentification disproportionately difficult.

In CHIC the hospital/investigator acting as data providers will carry out deidentification on-site before sending deidentified patient data to CHIC; the data will then be subject to a further round of encryption by the CDP, prior to transfer to the CHIC infrastructure. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the sensitive data to be protected.

The CHIC TTP alone holds the key necessary to re-link a given coded and deidentified data set with the second coded label (generated by the CDP during secondary encryption), to the original code attached to the data set by the data provider.

Sensitive (personal data)/Special categories of data

Sensitive personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health (including genomic data) or sex life. The processing of sensitive data is only allowed in case of certain exceptions explicitly stated by the national laws of the Member State.

Storage

Storage of personal data is allowed by the Data Protection Directive 95/46/EC. But when the purpose of processing is achieved and the data are not required any more for that particular purpose, personal data must be rendered anonymous or must be destroyed. Most national laws allow personal data to be stored for a longer term, provided that this is in order to use the data exclusively to carry out scientific research or statistics. Nevertheless, some national laws impose supplementary conditions or formalities in order to allow longer storage.

Technical and organisational measures

Organisational measures, together with technical measures, must ensure an appropriate level of security of the data processing, taking into account the state of the art and the costs of their implementation relative to the risks inherent in the processing and the nature of the data to be protected. Appropriate organisational measures shall be taken by the controller against accidental loss, destruction or alteration of, or damage to, personal data and against unauthorized or unlawful processing of personal data in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. The controller must, where processing is carried out on his/her behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures. Such appropriate organisational measures to ensure the confidentiality, integrity and accuracy of processed data should include for example:

- control of the entrance to installations
- control of data media
- memory control
- control of utilization
- access control
- control of communication
- control of data introduction
- control and securing of data transmission
- availability control

Such technical and organisational measures have to be taken by all the CHIC-participants processing patient data; other relevant required measures are set out in Annex B of the CHIC End User Agreement.

Third Party

A third party is a natural or legal person, public authority, agency or any other body other than the patient, the controller, the processor or persons who, under the direct authority of the controller or the processor, are authorised to process the data. With regard to CHIC, third parties will be all the other persons and bodies who have no authorisation from the CDP to process the data.

Transfer

Transfer of data means the transmission of CHIC data from one data controller to another.

Trusted Third Party

The role of Trusted Third Party in CHIC is performed by the CHIC TTP, an independent security authority, which has no interest in the content of the processed data and can therefore be trusted by all participants of the CHIC project. The Trusted Third Party will hold the pseudonymisation key (cross table) needed to link the double-encrypted CHIC data set to the initial deidentified data sets provided by the data providers. The involvement of the TTP guarantees that a CHIC data set can only be linked back to the original patient by the data provider institution treating the patient, in the exceptional circumstances defined in these Framework Terms.

Annex B

Technical and organisational measures

(Version 1.0, March 2014)

The CDP and the CHIC end user will take appropriate technical and organisational measures to protect the CHIC data against misuse and loss, in accordance with European data protection rules, including all necessary and reasonable precautions:

- to prevent unauthorised persons from gaining access to data processing systems with which the data are processed or used (physical access control),
- to prevent data processing systems from being used without authorisation (denial of use control),
- to ensure that persons entitled to use a data processing system can gain access only to the data to which they have a right of access, and that the data cannot be read, copied, modified or removed without authorisation in the course of processing or use and after storage (data access control),
- to ensure, including through use of secure encryption, that the data cannot be read, copied, modified or removed without authorisation during electronic transmission, transport or storage and that it is possible to examine and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged (data transmission control),
- to ensure that it is possible retrospectively to examine and establish whether and by whom the data have been inputted into data processing systems, modified or removed (input control),
- to ensure that the data being processed on commission are processed solely in accordance with the directions of the controller (contractual control),
- to ensure that the data are protected against accidental destruction or loss (availability control),
- to ensure that other (non-CHIC) data collected for different purposes is processed separately (separation rule).

Annex C

ACCESS AUTHENTICATION FORM

(Version 1.0, March 2014)

I, the undersigned Dr. Kostas Marias, (title) born on the 29th October 1972 in Athens Greece and working on the project called CHIC on behalf of FORTH (name of relevant CHIC partner institution) declare by this Access Authentication form, I am authorised to have access to the CHIC data.

I have read, I understand and I agree to observe the conditions as stated in the agreement as well as the General Framework Terms - which forms a part of this document (Version 1.0, March 2014).

I understand that two original copies of this agreement will be produced and will be kept by me and the CDP respectively.

Signature of employee: Konstantinos Marias

Date and Place: 5/8/2014 Heraklion, Crete, Greece

Annex C

ACCESS AUTHENTICATION FORM

(Version 1.0, March 2014)

I, the undersigned ...Mrs......Georgia....Kanli.........., (title) born on the ..31/03/88.........., in...Thessaloniki...Greece and working on the project called CHIC on behalf of .........F..O...R..T..H.... (name of relevant CHIC partner institution) declare by this Access Authentication form, I am authorised to have access to the CHIC data.

I have read, I understand and I agree to observe the conditions as stated in the agreement as well as the General Framework Terms - which forms a part of this document (Version 1.0, March 2014).

I understand that two original copies of this agreement will be produced and will be kept by me and the CDP respectively.

Signature of employee: ....

Date and Place: ....05/08/2014..............., Heraklion, Crete, Greece

Annex C

ACCESS AUTHENTICATION FORM

(Version 1.0, March 2014)

I, the undersigned GEORGIOS ZACHARIOUDAKIS (Mr) born on the 22 APRIL 1978 in HERAKLION, GREECE and working on the project called CHIC on behalf of FORTH declare by this Access Authentication form, I am authorised to have access to the CHIC data.

I have read, I understand and I agree to observe the conditions as stated in the agreement as well as the General Framework Terms - which forms a part of this document (Version 1.0, March 2014).

I understand that two original copies of this agreement will be produced and will be kept by me and the CDP respectively.

Signature of employee:

Date and Place: 28 JULY 2014 - HERAKLION, GREECE

Annex C

ACCESS AUTHENTICATION FORM

(Version 1.0, March 2014)

I, the undersigned Stelios Sfakianakis, (title) born on the 06/01/1974, in Heraklion, Greece and working on the project called CHIC on behalf of FORTH declare by this Access Authentication form, I am authorised to have access to the CHIC data.

I have read, I understand and I agree to observe the conditions as stated in the agreement as well as the General Framework Terms - which forms a part of this document (Version 1.0, March 2014).

I understand that two original copies of this agreement will be produced and will be kept by me and the CDP respectively.

Signature of employee: ....

Date and Place: 28/07/2014, Heraklion, Greece

Annex C

ACCESS AUTHENTICATION FORM

(Version 1.0, March 2014)

I, the undersigned ELEFTHERIOS KONTOPODIS (title) born on the 26-10-1981, in ATHENS - GREECE and working on the project called CHIC on behalf of FORTH declare by this Access Authentication form, I am authorised to have access to the CHIC data.

I have read, I understand and I agree to observe the conditions as stated in the agreement as well as the General Framework Terms - which forms a part of this document (Version 1.0, March 2014).

I understand that two original copies of this agreement will be produced and will be kept by me and the CDP respectively.

Signature of employee: ....

Date and Place: 29 - 07 - 2014 HERAKLION

Annex C

ACCESS AUTHENTICATION FORM

(Version 1.0, March 2014)

I, the undersigned ....Georgios.....Manikis....., (title Mr) born on the .06/04/1979.., in....Athens, Greece and working on the project called CHIC on behalf of FORTH declare by this Access Authentication form, I am authorised to have access to the CHIC data.

I have read, I understand and I agree to observe the conditions as stated in the agreement as well as the General Framework Terms - which forms a part of this document (Version 1.0, March 2014).

I understand that two original copies of this agreement will be produced and will be kept by me and the CDP respectively.

Signature of employee: ....

Date and Place: ...Heraklion, Crete.......28/07/14

Annex C

ACCESS AUTHENTICATION FORM

(Version 1.0, March 2014)

I, the undersigned Eleftheria Tzamali (title) born on September 8th, 1975 in Athens and working on the project called CHIC on behalf of FORTH declare by this Access Authentication form, I am authorised to have access to the CHIC data.

I have read, I understand and I agree to observe the conditions as stated in the agreement as well as the General Framework Terms - which forms a part of this document (Version 1.0, March 2014).

I understand that two original copies of this agreement will be produced and will be kept by me and the CDP respectively.

Signature of employee: ....

Date and Place: 29/07/2014, Heraklion-Crete

Annex C

ACCESS AUTHENTICATION FORM

(Version 1.0, March 2014)

I, the undersigned Vangelis Sakkalis, (title) born on the 22th May 1975 in Athens and working on the project called CHIC on behalf of FORTH (name of relevant CHIC partner institution) declare by this Access Authentication form, I am authorised to have access to the CHIC data.

I have read, I understand and I agree to observe the conditions as stated in the agreement as well as the General Framework Terms - which forms a part of this document (Version 1.0, March 2014).

I understand that two original copies of this agreement will be produced and will be kept by me and the CDP respectively.

Signature of employee: ....

Date and Place: 28/7/2014, Heraklion