FARMAINDUSTRIA´S STANDARD CODE ON PERSONAL DATA PROTECTION IN CLINICAL RESEARCH AND PHARMACOVIGILANCE

Registered at the Spanish Data Protection Agency Registry by means of the decision dated 17 June 2009.

This text is the non official translation of the Spanish version of the text Registered at The Spanish Data Protection Agency Registry. In case of disagreement, the Spanish version shall always prevail.

CONTENT

1

INTRODUCTION

1. INTRODUCTION.

FARMAINDUSTRIA is the national association for the pharmaceutical industry in Spain. It groups together 211 associate laboratories, which account for approximately 85.1% of prescription medicinal product sales in Spain.

FARMAINDUSTRIA's mission as an association focuses on the following objectives:

- Collaborating with the Public Administrations in arranging a stable regulatory financial framework that drives balanced market growth, increases R&D activities and the development of the pharmaceutical industry.
- Strengthening the public perception of the pharmaceutical Industry and its medicinal products, informing people, opinion leaders and public officials of the value that medicinal products contribute to our social progress and quality of life.
- Providing value added services to members companies in relation to information, assessment and business collaboration,
- Representing the Spanish pharmaceutical Industry at both, national and international level.

Within the framework of such objectives, FARMAINDUSTRIA created a working group devoted to the analysis of the application of personal data protection legislation in the Spanish pharmaceutical industry. This group focused on the processing of personal data in clinical research and pharmacovigilance activities.

In relation to clinical research, one of the conclusions of the analysis conducted was that there were various levels of access to subject data[1] by the laboratories, some knowing the subject's identity and others not. Furthermore, the laboratories that processed data without the subject's identification data, did not have dissociation procedures based on a unified approach throughout the industry.

In the case of pharmacovigilance, there are various data compilation scenarios, depending on the person who reports an adverse event i.e. the consumer himself, his legal representative, a relative, a healthcare professional or anyone other than the consumer of the medicinal product. As a result of this large number of scenarios, the procedure in order to obtain informed consent needs to be formalised. Law 29/2006, of 26 July 2006 on guarantees and the rational use of medicinal products and medical devices, however, enables, within the field of pharmacovigilance, the processing of personal data without the need for consent and therefore only the duty to inform will apply.

Clinical research and pharmacovigilance are basic to scientific progress. They are highly regulated activities where there are standard procedures that offer the subject the best assurances in relation to the medicinal products prescribed and medical supervision of the treatment.

FARMAINDUSTRIA considers that the pharmaceutical industry's standardisation effort may be extended to the processing of personal data in clinical research and pharmacovigilance through a standard code that provides for the multiple

[1] In this document, the term subjects is used to refer to healthy people or patients participating in clinical trials or other clinical research studies.

scenarios that may arise in the day-to-day operation of a laboratory. This standard code would be applicable in the following instances:

1. Clinical Research using dissociated data.
2. Clinical Research using personal data.
3. Pharmacovigilance using dissociated data.
4. Pharmacovigilance using personal data.

The advantages of a standard code are evident since it is impossible for the legislator to regulate all circumstances in a particular sector while an organic law and even regulations do not aim to go into that level of detail. The standard code becomes the ideal instrument to obtain a consistent approach to the sector application of the Law on Data Protection, enhance compliance and reduce the level of uncertainty with respect to its interpretation.

Of the specific advantages of the approval of the Clinical Research and Pharmacovigilance Standard Code, the following are noteworthy:

- Pharmaceutical laboratories will have Action Protocols that will enable the application of a consistent approach to the processing of subject data on clinical research projects and in relation to pharmacovigilance.
- Such protocols will provide for instances of clinical research and pharmacovigilance using both personal and dissociated data.
- The subjects involved in a clinical study or any other clinical research process will have the utmost assurance with respect to the processing of their data.
- In relation to pharmacovigilance, the standardisation effort will enable a consistent and appropriate response to the multiple scenarios that may arise when reporting adverse events and obtaining informed consent, where necessary, offering maximum legal guarantees to consumers, doctors and laboratories.
- For the laboratories, the level of uncertainty will decrease in both interpreting the Law on Data Protection and its Regulations and applying it in the most usual instances of the day-to-day operation of the pharmaceutical industry.
- The Spanish pharmaceutical industry will offer market players and product consumers, in particular, an image of unity, sensitivity, corporate effort and respect for people's basic rights in the processing of the personal data of those involved in a clinical trial or in any other clinical research or pharmacovigilance process, in accordance with current legislation.

In short, both subjects involved in trials and studies and consumers will benefit from the guarantees offered by a consistent personal data protection regime since it provides legal certainty which would otherwise be difficult to secure, avoids the proliferation of heterogeneous procedures or regimes and facilitates the exercise of their rights vis-à-vis the laboratories that have adhered to this Standard Code. This will help to further enhance confidence in an industry that has at all times been extremely meticulous in the processing of this type of data.

The sum of these advantages turns the Standard Code into a distinctive feature of those laboratories that voluntarily adopt it.

2

LEGAL FRAMEWORK

2. LEGAL FRAMEWORK.

- Organic Law 15/1999, of 13 December 1999, on Personal Data Protection (hereinafter LOPD).

- Law 29/2006, of 26 July 2006, on guarantees and the rational use of medicinal products and medical devices.

- Law 41/2002, of 14 November 2002, which basically governs patient autonomy and the rights and obligations attached to clinical information and documentation.

- Royal Decree 1720/2007, of 21 December 2007, approving the Enabling Regulations of Organic Law 15/1999, of 13 December 1999, on Personal Data Protection (hereinafter RLOPD).

- Royal Decree 1345/2007, of 11 October 2007, governing the process for the authorisation, registration and conditions for supplying industrially manufactured medicinal products for human use.

- Royal Decree 1344/2007, of 11 October 2007, on Pharmacovigilance of medicinal products for human use.

- Royal Decree 223/2004, of 6 February 2004, on clinical trials on medicinal products for human use

- Order SCO/256/2007, of 5 February 2007, establishing the principles and detailed guidelines of good clinical practice and the requirements for authorising the manufacture or import of investigational medicinal products.

- Order SCO/362/2008, of 4 February 2008, amending Order SCO/256/2007, of 5 February 2007, establishing the principles and detailed guidelines of good clinical practice and the requirements for authorising the manufacture or import of medicinal products for human use.

- Volume 9 A of The Rules Governing Medicinal Products in the European Union. Guidelines on Pharmacovigilance for medicinal products for human Use.

- Guideline for Good Clinical Practice (CPMP/ICH/135/95).

- Good practice in Pharmacovigilance for the pharmaceutical industry in relation to medicinal products for human use.

- Instructions of the Spanish Data Protection Agency and Guidelines of the Spanish Agency of Medicinal products and Medical Devices (AEMPS).

3

DEFINITIONS

3. DEFINITIONS.

For the purposes of this Standard Code, the following definitions will be taken into account:

Adverse event: Any untoward medical occurrence in a patient or subject treated with a product which does not necessarily have a causal relationship with this product.

Affected or interested party: This is the individual owner of the data being processed.

Auditor: This refers to any individual or legal entity responsible for the independent and systematic examination of the activities and documents related to a clinical research project, in order to determine whether the activities assessed in relation to the study, were performed and the data were correctly recorded, analysed and reported in accordance with the study Protocol, Standard Operating Procedures (SOP), the rules on Good Clinical Practice and regulatory requirements.

Hospital sites (or medical institution). This is any private or public entity or medical or dentistry facility or agency where clinical studies are conducted. The Centre is responsible for the "Clinical Investigation File" (CIF) and as such, should, inter alia, report the creation of the CIF to the Spanish Personal Data Protection Agency (AEPD) prior to its creation.

Assignment or communication of data: Data processing that entails disclosure to someone other than the interested party.

Collaborator: any member of the clinical trial team, designated and supervised by a researcher at an investigation centre to carry out significant procedures and/or take major decisions connected with the trial (eg, associate residents, persons with investigation grants).

Research Ethics Committee: This is an independent body, made up of healthcare professionals and non-healthcare members, responsible for overseeing the protection of the rights, safety and wellbeing of the subjects involved in a trial and offering public assurance in this respect by expressing an opinion on the trial protocol, the suitability of the researchers and the appropriateness of the facilities and the methods and documents to be used to inform the trial subjects in order to obtain their informed consent.

Consent of the interested party: This refers to expressions of consent, free, unequivocal, specific and informed, through which the interested party consents to the processing of his personal data.

Informed consent: decision, which must be written dated and signed, to take part in a clinical trial, taken freely by any person capable of giving consent after being duly informed and appropriately documented of its nature, significance, implications and risks. If the subject is unable to write, oral consent in the presence of at least one witness may be given in exceptional cases

Where the trial subject is not capable to give consent, the decision must be taken by his legal representative.

Consumer: This is any person other than the healthcare professional who experiences an adverse event during the use or utilisation of any product marketed by a pharmaceutical laboratory.

Case Report Form: A printed, optical or electronic document designed to record all of the protocol required information to be reported to the sponsor on each study subject.

Personal data: Any numerical, alphabetical, graphic, photographic, acoustic or any other type of information concerning identified or identifiable individuals.

Identification data: Any information concerning individuals that enables their identity to be known. The following are considered identification data:

- Name.
- Surname.
- Subject's initials.
- Telephone number.
- Address.
- National ID number, Social Security number, Clinical Record number or similar, assigned by the Administration.

Personal data related to health: Information concerning an individual's past, present and future physical or mental health. In particular, information related to a person's health includes data on his disability rate and genetic information.

Dissociated data: Data that does not allow the affected or interested party to be identified.

Party in charge of processing: The individual or legal public or private entity or administrative body that, alone or together with others, processes personal data on behalf of the party responsible for the processing of the file as a result of the existence of a legal relationship linking them and defines the scope of action for the provision of a service.

Those entities without a legal personality operating as distinct subjects may also be responsible for the processing.

Clinical trial: This refers to all investigation conducted on human beings in order to determine or confirm the clinical, pharmacological and/or other pharmaco-dynamic effects and/ detect adverse reactions and/or study the absorption, distribution, metabolism and elimination of one or several Investigational medicinal Products in order to determine their safety and/or efficiency.

Clinical study: This refers to a clinical trial, an observational post-authorisation study or other types of observational studies in which no treatment is administered to patients.

Observational post-authorisation study: This is any observational clinical or epidemiological clinical study performed during the marketing of a medicinal product according to the conditions authorised in its technical file or under normal conditions of use, where the medicinal product or medicinal products involved are the basic exposure factor being investigated.

File: All organised sets of personal data, enabling access to data under certain criteria, irrespective of the form or manner of their creation, storage, organisation and access.

Clinical record: The set of documents containing data, status reports and the clinical evolution of a patient over the medical process.

Inspection: The act by a competent authority of conducting an official review of documents, facilities, records, quality assurance arrangements and any other resources that are deemed by the competent authorities to be related to the clinical trial and that may be located at the site of the trial, at the sponsor's and/or contract research organisation facilities, or at other establishments which the competent authority sees fit to inspect.

Investigator: A doctor or person exercising a profession recognised as enabling him to conduct investigation thanks to his scientific training and healthcare experience. The investigator is responsible for the performance of the clinical trial at a centre. If the trial is carried out by a team, the investigator is responsible for the team and may refer to himself as the principal investigator.

Laboratory: All entities or pharmaceutical companies that manufacture and/or market medicinal products.

Investigator's Brochure: A compilation of the clinical and non-clinical data on the Investigational medicinal products which are relevant for the study of the product in human subjects.

Investigational medicinal product: A pharmaceutical form of an active substance or placebo being tested or used as a reference in a clinical study, including products already with a marketing authorisation, but used or assembled (formulated or packaged) in a way different from the authorised form, or when used for an unauthorised indication, or when used to gain further information about the authorised used.

Monitor: A qualified professional with the necessary clinical competence, chosen by the sponsor, who is responsible for the direct follow-up of the trial. He acts as a link between the sponsor and the principal investigator when they are not the same person.

Contract Research Organization (CRO): An individual or legal entity contracted by the sponsor to perform the sponsor's clinical study-related functions or duties or contracted by the laboratory for pharmacovigilance activities.

Other observational studies: These studies differ from clinical trials and post-authorisation studies. Their aim is to analyse the distribution of disease and its determinants in specific populations. This would be the case, for example, of the study of the incidence of slight arterial hypertension in the adult population of a certain location.

Other reporters: Those persons who, although not healthcare professionals, are not the consumer, and who notify the pharmacovigilance unit of the adverse event suffered by the consumer, such as, for example, the consumer's relatives or close friends.

Dissociation procedure: All processing of personal data that enables dissociated data to be obtained.

Standard Operating Procedures (SOP): Detailed written instructions to achieve uniformity of the performance of a specific function.

Product: The term product includes medicinal products, medical devices and nutritional products (therapeutic diet, foods and enteral nutrition).

Healthcare professional: These are doctors, pharmacists, dentists, nurses and other healthcare professionals who are required to report suspicions concerning the adverse reaction of some product marketed by a pharmaceutical laboratory.

Sponsor: An individual, company, institution or organisation, of Spanish nationality, responsible for the initiation, management and/or financing of a clinical study. In the case of international clinical studies, for the purposes of this Code, the entity acting in its name and on its behalf in Spain will be considered the sponsor.

Protocol: A document that describes the objectives, design, methodology, statistical considerations and organisation of a study. The term protocol refers to the original protocol, successive versions of the protocol and protocol amendments.

Adverse reaction: Any response to a medicinal product that may be harmful or unintentional and which arises at doses normally applied to human beings as prophylaxis or in the diagnosis or treatment of disease or the restoration, correction or modification of physiological functions. This term also includes all adverse clinical consequences deriving from dependence, abuse and the incorrect use of medicinal products, including those caused by the use under non-authorised conditions and medication errors.

Consumer's legal representative: A person who, on behalf of a disabled person or minor, notifies the pharmacovigilance unit of the event experienced by the consumer.

Party responsible for the file or processing: An individual or public or private legal entity or administrative body, that alone or together with others, decides on the purpose, content and use of processing although he does not conduct it.

Study subject: A healthy individual or patient who participates in a clinical trial or other clinical research studies.

Data processing: Any technical operation or procedure, automated or other, that enables the collection, recording, storage, preparation, modification, enquiry, use, cancellation, blocking or suppression and assignment of the data resulting from communications, enquiries, interconnections and transmissions.

Pharmacovigilance unit: This is the department responsible for receiving reports of, recording and managing adverse events.

4

SCOPE OF APPLICATION

4. SCOPE OF APPLICATION.

4.1 Subjective scope of application.

- This Standard Code will be applicable to:

  a) The pharmaceutical laboratories that are associate members of Farmaindustria and that expressly declare their adherence to this Standard Code.

  b) The pharmaceutical laboratories that are not associate members of Farmaindustria and that expressly declare their adherence to this Standard Code.

  c) CROs that provide services on account of pharmaceutical laboratories for the studies in which pharmaceutical laboratories are the sponsors and that expressly declare their adherence to this Standard Code. Also, those CROs that provide pharmacovigilance services to pharmaceutical laboratories.

  Since a clinical research involves other professionals such as the Investigator, Hospital Centre, Monitor, Auditor and collaborators, the sponsors and CRO that have adhered to the Standard Code will ensure that the other parties involved in a clinical research collaborate with them in complying with the obligations of the present Standard Code.

  Investigators, hospital sites, monitors, auditors and other collaborators will therefore be asked to cooperate with the sponsors and CRO that have adhered to the Standard Code in fulfilling their obligations, ensuring the confidentiality of the data which they may access in accordance with current legislation and at all times subject to the duty of secrecy inherent in their profession.

- The entities included in the specific scope of application should comply with the present Standard Code and the provisions of personal data protection legislation insofar as they process personal data in the conduct of their activities. In this respect, special attention should be paid to Organic Law 15/1999, of 13 December 1999, on personal data protection and Royal Decree 1720/2007, of 21 December 2007, whereby the enabling regulations were approved of Organic Law 15/1999, of 13 December 1999, on personal data protection.

4.2 Objective scope of application.

- **Clinical research.-** The sponsors of clinical trials may opt to process the personal data of the subjects identified or to apply a dissociation procedure that ensures that the data to be processed do not allow the trial subject to be identified. This Standard Code will be applicable in both cases. If the sponsors decide to process subjects' personal data, the scope of application will extend to all kinds of carrier media and types of processing, automated or other.
  This Standard Code may also be applied to observational post-authorisation studies and other types of observational studies.

- **Pharmacovigilance.**- This Standard Code will also be applicable to the processing by pharmaceutical laboratories of consumer data in pharmacovigilance units, stored in any form for any kind of processing, automated or other. Data will relate to the adverse events that may be connected with the consumption of the products marketed by the pharmaceutical laboratories.

- **Files.-** The personal data or dissociated data files in both clinical research and pharmacovigilance are also covered by this Standard Code.

  - **Clinical Investigation File (CIF).-** this is the file of the health centre where the trial is conducted. This file is made up of the entire subject's clinical documentation and the data generated as a result of the study. Such data are processed for the overall management of the study.

  - **Case Report Form File (CRFF).-** this is the laboratory's file (trial sponsor). This file comprises all the protocol required information for the study. The purpose of the processing of the data included in the CRFF consists of assessing the findings of the study and drawing the appropriate conclusions.

  - **Pharmacovigilance file.-** this is the laboratory file that contains any suspicions concerning adverse reactions notified by healthcare professionals and adverse events experienced by consumers of the laboratories' products in order to analyse the safety of such products and report to the healthcare authorities.

- **Notification and registration.-** The obligations of notification and registration provided in Article 26 of the LOPD and Articles 55 et seqq. of the enabling regulations are applicable to the personal data files under this Standard Code. Registration is an indispensable requirement in order to adhere to this Standard Code.

4.3 Legitimation of FARMAINDUSTRIA.

- FARMAINDUSTRIA is recognised as the pharmaceutical industry's representative in Spain thanks to the large number of laboratories which it groups together and which account for around 85.1% of prescription medicinal product sales in Spain.

- This Standard Code has been subject to discussion in working groups devoted to processing personal data, clinical research and pharmacovigilance and approved by Farmaindustria's governing bodies.

4.4 Entry into effect.

- This Standard Code will come into effect as from the date of its registration at the Data Protection General Registry.

- The laboratories and CRO will be bound by this Standard Code as from the time of their adherence to the same following its registration with the Data Protection General Registry.

5

ACTION PROTOCOLS

5.1. ACTION PROTOCOL – CLINICAL TRIALS AND OTHER CLINICAL RESEARCHES.

5.2. ACTION PROTOCOL – PHARMACOVIGILANCE.

5.3. ACTION PROTOCOL – ARCO RIGHTS.

5.4. ACTION PROTOCOL – SELF-REGULATION SYSTEM.

5.1- ACTION PROTOCOL ON CLINICAL TRIALS AND OTHER CLINICAL RESEARCHES.

I. Introduction and scope of application

II. Initiation of a Clinical research

III. Clinical research using dissociated data.

1.- Introduction
2.- Development and control of the clinical study
3.- Dissociation procedure
4.- Adverse events
5.- Termination of the study
6.- Third-party access to data
7.- Security measures
8.- International transmission
9.- ARCO rights

IV- Clinical research using personal data

1.- Introduction
2.- Development and control of the clinical study
3.- Adverse events
4.- Termination of the study
5.- Third-party access to data
6.- Security measures
7.- International transmission
8.- ARCO rights

Annex I: Informed consent with personal data processed exclusively by the centre.

Annex II: Informed consent with personal data received / processed by the sponsoring laboratories.

Annex III: Clinical Investigational File

Annex IV: Confidentiality agreement – Parties involved with access to personal data

Annex V: Case Report Form File (CRFF)

Annex VI: Clause on personal data processing – Party responsible for processing

5.1- ACTION PROTOCOL ON CLINICAL TRIALS AND OTHER CLINICAL RESEARCHES.

I. INTRODUCTION AND SCOPE OF APPLICATION.

Medicinal products are a substance or combination of substances that are presented as having properties to treat or prevent disease in humans or that may be used in humans or dispensed to humans in order to restore, correct or modify physiological functions through pharmacological, immunological or metabolic action, or arrive at a medical diagnosis (Article 8 of Law 29/2006, of 26 July 2006, on Guarantees and the Rational Use of Medicinal Products and Medical Devices).

For a medicinal product to be authorised by the healthcare authorities it is essential to evaluate the documentation containing the entire investigation conducted by the laboratory.

The pre-clinical and Clinical research of a new medicinal product starts with "in vitro" studies, studies in animals and subsequently, its clinical development is carried out in humans through clinical trials.

According to the definition in Article 58 of Law 29/2006, of 26 July 2006, on Guarantees and the Rational Use of Medicinal Products and Medical Devices (hereinafter Law 29/2006), clinical trials are all investigations conducted on human subjects intended to verify the clinical, pharmacological and/or other pharmaco-dynamic effects and/or detect adverse reactions and/or to study the absorption, distribution, metabolising and elimination of one or various investigational medicinal products in order to determine their safety and/or effectiveness.

Clinical trials are universal investigation instruments which enable the discovery of new medicinal products. In order to ensure that clinical trials are valid, they are conducted in accordance with the so-called Guideline for Good Clinical Practice, a standard international operating procedure, providing public assurance that the rights, safety and the wellbeing of trial subjects are protected and ensuring that the study data are credible.

The *Action Protocol on Clinical Trials and other Clinical Researches will* be applicable to the clinical research sponsors and CROs that have adhered to Farmaindustria's Standard Code.

The sponsors and CROs adhering to the Standard Code will ensure that the other agents involved in a Clinical research collaborate with them in fulfilling the obligations contained in the present Action Protocol and the rest of the Standard Code.

In this way, investigators, hospital sites, monitors, auditors and all their collaborators will be asked to cooperate with the sponsors and CROs that have adhered to the Standard code in fulfilling their obligations, by ensuring the confidentiality of the data accessed in accordance with current legalisation, at all times observing the duty of secrecy inherent in their profession.

The Protocol is structured into three main sections: (II) Initiation of a Clinical Research, (III) Clinical Research using dissociated data and (IV) Clinical Research using personal data.

The section on "Initiation of a Clinical Research" may be considered common to clinical research using dissociated data and clinical research using personal data, unless otherwise indicated.

II. INITIATION OF A CLINICAL RESEARCH.

1. Stage prior to the initiation of a Clinical Research

1.1. Clinical trial

A clinical trial starts with the preparation of a Protocol by the sponsor. The sponsor is that individual, company, institution or organisation of Spanish nationality, that takes responsibility for the initiation, management and/or financing of a clinical trial. For international studies and for the purposes of this document, the entity acting in his name and on his behalf in Spain will be considered the sponsor.

The protocol is a document that describes all aspects of the study and that together with the rest of the documentation connected with the study contains at least the following information:

- Identification of the protocol (code assigned by the sponsor).
- Clinical trial title.
- Identification of the sponsor.
- Centres where the trial is expected to be conducted.
- Trial Justification and background.
- Design, including how subjects will be randomised.
- Main objective and other objectives and aims of the study.
- Experimental medicinal product and control: doses, pharmaceutical form, route of administration, therapeutic group, treatment period.
- Trial subjects and total number of patients.
- Assessment of efficacy and safety: main and secondary variables of the study.
- Statistical analysis.
- Ethical considerations.
- Timeline and expected completion date.
- Access to the source documents of the study for monitoring, audit and inspections.
- Quality control and guarantee.
- Financing and insurance.
- Policy on the publishing of results.
- Information sheet for study subjects and informed consent form.

Clinical trials may only be conducted at suitable centres. The sponsor will therefore be required to carry out a series of checks to ensure that the investigator and his team are suitably qualified and that the centre is adequate in that it has the appropriate facilities and necessary resources over the expected duration of the study for it to be correctly and safely completed.

Similarly, the sponsor's selection of investigator is very important. The principal investigator is the physician or person who carries on a profession recognised to conduct research thanks to his scientific training and experience in providing the requisite healthcare and who takes responsibility for the clinical study.

Furthermore, the sponsor is required to provide to the investigator the basic clinical information available on the investigational product. In the course of the clinical trial, this obligation will persist and the sponsor should inform the investigator of any significant information connected with the investigational product.

Checks of the adequacy and suitability of the centre and investigator and the information obligations referred to above are normally conducted by a monitor at the site where the clinical trial will be conducted during the so-called visit prior to initiation.

The monitor is a qualified professional with the necessary clinical competence, who is chosen by the sponsor and is responsible for the direct monitoring of the study. He is a link between the sponsor and investigator when they are not the same person.

Following the completion of the protocol and mandatory checks and the discharge of the information obligations, in order to initiate the trial, it will be necessary to obtain the favourable opinion of the Clinical research Ethics Committee (hereinafter CEIC) and the authorisation of the Spanish Agency of Medicines and Medical Devices (hereinafter AEMPS).

Set out below is an overview of the procedures established to request the aforementioned opinion and authorisation, in accordance with Royal Decree 223/2004, of 6 February 2004, on clinical trials with medicinal products.

CEIC opinion

The procedure will begin with the sponsor's application to the CEIC. The application should be accompanied by at least: a) the protocol; b) the investigator's brochure; c) standard informed consent forms; d) an information sheet for the trial subject; e) a copy of the insurance policy certificate; f) the study's financial agreement; and g) the investigator's commitment to conduct the study in accordance with the Guideline for Good Clinical Practice.

Once the application has been filed and accepted, together with the mandatory documents to be provided, the CEIC will have 60 calendar days to report its opinion and the grounds on which it is based to the sponsor and the AEMPS.

The period indicated will be 90 calendar days when the clinical trial is connected with gene therapy, somatic cell therapy or when it contains genetically modified organisms. In this latter case, the period may be extended for a further 90 calendar days when the opinion has to be issued by an expert committee.

For clinical trials connected with xenogenic cell therapy, there will be no limit on the time the CEIC can take to issue an opinion.

The CEIC will issue a single favourable opinion irrespective of whether we are dealing with single or multicentre clinical trials.

Authorisation of AEMPS

Following the application filed with the CEIC, the sponsor will apply in writing to the AEMPS for authorisation. Together with the application, the sponsor should provide certain documents such as: a) the trial protocol; b) the investigator's brochure; c) the

trial subject's information sheet; and d) a dossier concerning the investigational product.

Once the application has been filed and accepted together with the documents provided, the AEMPS will have 60 calendar days to object to the clinical trial. If no objections are raised in that period, authorisation will be understood to have been granted provided that the AEMPS has received the favourable opinion of the CEIC and the agreement of the management of the centre where the trial is to be conducted.

Nonetheless, the special procedure, provided in Royal Decree 223/2004, of 6 February 2004, on clinical trials with medicinal products, which requires a positive decision from the AEMPS within 60 calendar days will be followed. That procedure will be applicable in some of the following cases: a) when the medicinal product qualifies as an investigational product for human use; b) when the AEMPS has reported objections to the sponsor in accordance with the paragraph above; c) when dealing with clinical trials involving genetic therapy, somatic cell therapy or genetically modified organisms.

For clinical trials involving xenogenic cell therapy, the AEMPS will be subject to no time restrictions to object to, authorise or reject the clinical trial.

Centre agreement

In order to initiate the clinical trial, in addition to the CEIC's opinion and the authorisation of the AEMPS, the centre must agree to the trial through an express consent document and a contract with the Sponsor containing legal and economic clauses. Some Autonomous Regions have prepared standard contracts to be used by their centres.

1.2. Other clinical studies

Unlike in clinical trials, where generally the aim is to identify new therapeutic findings, it may be necessary to conduct studies of medicinal products under authorised marketing conditions in order to verify their performance when they are used in habitual clinical practice and identify, characterise or quantify possible risks associated with their use. These studies, named post-authorisation studies, are mainly aimed at determining the safety and efficacy of the medicinal product, identifying departures from usual practice or verifying on a long-term basis that patients continue to present the expected results.

The content of the protocol and selection of centres and investigators are very similar to those described in the section on clinical trials. However the authorisation procedure for observational post-authorisation studies is established in Royal Decree 1344/2007, of 11 October 2007, on pharmacovigilance of medicinal products for human use.

1.2.a. Observational post-authorisation studies

A post-authorisation study is any observational clinical or epidemiological study conducted once a medicinal product has been marketed under the conditions authorised in its Summary of Product Characteristics or under normal conditions of use, and where the medicinal product or products involved are the basic exposure factor investigated.

The Sponsor should send the study protocol to the AEMPS for it to report the procedures to be followed in each case.

When the conduct of the observational post-authorisation study is a condition laid down at the time a medicinal product is authorised or is a requirement of the regulatory authorities with a view to clarifying concerns about the medicinal product's safety or forms part of the risk management plan that should be undertaken by the laboratory marketing a medicinal product, only AEMPS authorisation will be required.

For other observational post-authorisation studies, the favourable opinion of the CEIC will be required together with the authorisation of the regulatory authorities, as appropriate.

1.2.b. Other observational studies

These studies differ from clinical trials and post-authorisation studies. Their aim is to analyse the distribution of disease and its determinants in specific populations. This would, for example, be the case of the study of the incidence of slight arterial hypertension in the adult population of a specific location.

These studies are submitted to a CEIC for evaluation.

2. Collection of subject personal data.

The investigator will be responsible for selecting the subjects who will participate in the study. Any reference to the investigator will also be understood to refer to that investigator's collaborator team[2].

The main sources which the investigator may use to select subjects for the study are as follows:

1. Population visiting the principal investigator's and collaborators' surgery.
2. Patients referred from other centre departments or divisions.
3. Patients referred from other associate centres.
4. Subjects asking the investigator directly. In such cases, the subject learns of the trial through other subjects, clinical trial registers or as a result of specific actions to publicise the study and favour subject recruitment. The materials and procedures used in these actions should be evaluated and authorised by the CEIC.

The selection should be carried out in accordance with the criteria and guidance established in the protocol and in any event, will entail access by the principal investigator or his collaborators to the clinical registers of potential trial subjects in order to verify their eligibility on the basis of protocol requirements. The investigator who accesses clinical records is a professional qualified to follow the subject at healthcare level and therefore has access to such clinical records.

[2] Collaborator. Any member of the clinical trial team who is designated and supervised by the investigator in a research centre in order to carry out the relevant procedures and/or take major decisions connected with the trial (eg associates, residents, research fellows).

3. Informed consent.

Once the healthy individuals or subjects who are eligible to participate in the study have been identified, the investigator should fulfil a number of information obligations with respect to possible participating subjects in order to obtain their express consent.

Information

The investigator should inform the subject in a clear and comprehensible manner of the study's objectives, its risks and drawbacks and the conditions under which it will be conducted. In particular, the subject should be informed of the following aspects at least:[3]

- The trial involves research.
- The purpose of the trial.
- Trial treatments and possibility of the random assignment of each treatment.
- The procedures to be followed in the trial, including invasive procedures.
- The subject's responsibilities.
- Those aspects of the trial that are experimental.
- Risks and drawbacks for the subject and, where appropriate, for the embryo, foetus or lactating baby and which may be reasonably foreseen.
- Reasonably expected benefits.
- Alternative procedures or treatments available to the subject and their possible benefits and risks.
- Indemnity and/or available treatment for the subject in the event of any adverse effect connected with the trial.
- Forecast pro-rata of the payment due to the subject for his participation in the trial, if any.
- Reimbursement of foreseeable expenses, if any, to the subject for his participation in the trial.
- The subject's participation in the trial is voluntary and the subject may refuse to participate or withdraw from the trial at any time, without any penalty or loss of the benefits to which he may otherwise have been entitled.
- The monitors, auditors, CEIC and regulatory authorities will have direct access to the subject's clinical records in order to check the clinical trial procedures and/or data, without infringing on the subject's confidentiality, as permitted by law, and which, by signing the informed consent, the subject or his legal representative is authorising.
- The records that identify the subject will be confidential and, pursuant to local regulations, will not be publicly available. If the trial's results are published, the subject's identity will remain confidential.
- The subject or the subject's legal representative will at all times be informed of whether there is any new information that may affect his decision to continue participating in the trial.
- Contacts to obtain additional information on the trial and the rights of participating subjects and to contact in the event of lesions related to it.

[3] CPMP/ICH 135/95 Guideline for Good Clinical Practice.

- Foreseeable circumstances and/or reasons under which the subject's participation in the trial may end.
- Expected duration of the subject's participation in the trial.
- The approximate number of subjects involved in the trial.

Such information should be reported verbally to the subject of the study during an interview with the investigator or any of his collaborators. The subject will also receive this information in writing through a patient information sheet. The subject should have the necessary time to consider his participation and all questions must be addressed.

In a manner parallel to the information obligations deriving from clinical legislation, there are obligations concerning the information that should be provided to the patient in order to comply with current legislation on the protection of personal data when these are used in the study.

In trials involving personal data, the information sheet or accompanying document should expressly, accurately and unequivocally state the following:

- The existence of a file or processing of personal data, the reason why such data are being collected and the persons who may be the recipients of any information concerning the subject which has not been dissociated. For recipients outside the European Economic Area, in addition to their identification, it will be necessary to indicate the countries where they are located.
- The mandatory or optional nature of their replying to the questions raised.
- The consequences of obtaining information or refusing to provide it.
- The possibility of exercising ARCO rights. The instructions which are provided in this respect to subjects should agree with the action protocol for the observance of ARCO rights that form part of this Standard Code.
- The identity and address of the person responsible for the file or, if appropriate, his representative.
- If the sponsor has adhered to Farmaindustria's Standard Code, the subject may consult the content of the Standard Code in person or over the Internet at both Farmaindustria and the Spanish Data Protection Agency.

Consent

Consent should be expressly given and documented using the information sheet for the subject and the consent document.

It will be necessary to take into account the specific circumstances involved when the subject is a minor or a disabled adult.

- Minors.
  - The minor's legal representatives will give their consent to the minor's inclusion in the trial. If the minor is 12 years old or older, he should also provide his consent.

  - The minor should receive information appropriate to his condition from specialists with experience in dealing with minors.
  - His participation will entail the need to inform the Government Attorney of authorisations in relation to such clinical trial.

- Disabled adults.
  - Their legal representative will be whoever provides the necessary informed consent for the subject to participate in the trial.
  - When the subject's condition allows, he should also provide his consent.

In exceptional cases, there will be no need for the subject's consent. Such cases are strictly assessed under clinical legislation and should be provided for in the study documentation that has been approved by the CEIC.

It should be borne in mind that the consent given by subjects participating in the trial may be withdrawn at any time during the study with no need for the subject to expressly declare the reason and without such withdrawal having an adverse effect for that subject. This possibility is also applicable to minors and disabled adults in the event of the investigator perceiving that this is the minor's or disabled adult's intention.

Once consent has been obtained, the document will be kept in the centre's files and a copy will be given to the subject participating in the clinical trial.

The content of the consent document connected with personal data protection will vary depending on whether we are dealing with a Clinical research with personal data or a Clinical research with dissociated data.

In this respect, **Annex I and II** set out the minimum content of the consent document connected with data protection for Clinical research involving dissociated data and personal data, respectively.

III. CLINICAL RESEARCH USING DISSOCIATED DATA.

1. Introduction.

In order to prepare this section, data protection legislation has at all times been taken into account, i.e., Organic Law 15/1999, of 13 December 1999, on Personal Data Protection (hereinafter LOPD) and Royal Decree 1720/2007, of 21 December 2007, approving the enabling regulations of Organic Law 15/1999, of 13 December 1999, on Personal Data Protection, Law 29/2006, of 26 July 2006, on Guarantees and the Rational Use of Medicinal Products and Medical Devices and Royal Decree 223/2004, of 6 February 2004, governing clinical trials with medicinal products and Royal Decree 1344/2007, of 11 October 2007, governing the pharmacovigilance of medicinal products for human use.

If, when performing a clinical trial or observational study, the sponsor opts to work with dissociated data, the procedure to be followed is that described in this section.

This procedure will ensure that the process cannot be reversed since associating the codified data resulting from the application of the dissociation process with the subject's identification details would entail a disproportionate effort.

Any reference to the centre where the trial is conducted will be understood to also refer to the various centres where multi-centre trials are conducted. Similarly, any reference to the investigator will also be understood to refer to the investigator's collaborator team.

2. Management and Conduct of the Study

The investigator and his collaborators will carry out the actions laid down in the protocol and complete the case report forms (CRFs) using the clinical information generated as a result of the study. The investigator, as the person responsible for the data included in the CRFs, should sign these documents[4].

In the course of the study and in order to complete it, various agents may have contact with the investigator. Specifically, the investigator is required to enable and facilitate monitoring and auditing and possible inspection by the regulator.

Set out below is a list of such agents, their main responsibilities and legal position in relation to the personal data of the study participants.

- The Sponsor. The sponsor is the individual, company, institution or organisation responsible for the initiation, management and/or financing of a study. His responsibilities consist of:

  - Asking the CEIC for an opinion and the AEMPS or the Autonomous Regions involved for authorisation, depending on the type of study.
  - Free supply of the investigational medicinal product for human use (only for clinical trials).

[4] A CRF (Case Report Form), is a printed, optical or electronic document designed to collect and transmit to the sponsor all the information required under the protocol for each study subject.

- Establishing a guarantee and quality system through standard operating procedures (SOPs)[5].
- Ensuring that the study fulfils the provisions of the protocol and applicable clinical legislation.
- Signing the protocol and any of its amendments with the investigator.
- Selecting the most appropriate investigator.
- Designating a monitor to oversee the progress of the trial.
- During clinical trials, reporting to the healthcare authorities, investigators and CEIC any suspicions of any suspected unexpected serious adverse reactions. During observational post-authorisation studies, the sponsor should inform the competent healthcare authorities of any serious adverse reactions.
- Fulfilling requirements to report any major issues arising during the study to both the CEIC and the investigator.
- On clinical trials, providing economic compensation to subjects in the event of injury or death connected with the trial.
- Agreeing with the investigator the obligations in relation to data processing, preparation of reports and publication of results.

Communication between the sponsor and the investigator will in practice be channelled through the monitor. The sponsor will be authorised to establish direct communication with the investigator and may ask him to send copies of the CRF without the inclusion of the subject's identification details and by referring solely to the dissociation code.

The sponsor will in no event participate in collecting the personal data of the trial subjects and nor will he have access to the files and/or documents in which the investigator or Centre stores such data.

In short, the sponsor will at no time access the trial subjects' personal data.

Although the sponsor does not have access to the personal data of the subjects participating in the trial, he is responsible for deciding, inter alia, the criteria determining the subject's participation in the trial, the actions for informing the healthcare authorities, the guidelines for preparing the mandatory reports and, in short, for overseeing the way in which the trial as a whole is conducted.

In short, as set out in this Protocol, the sponsor establishes the guidelines for processing trial subjects' personal data. This means that although he does not have access to data, the sponsor is responsible for processing in relation to the Clinical Investigational File .

This does not entail any additional responsibilities other than those related to the duty of diligence. Therefore, as the sponsor holds no personal data, he will be unable to handle situations involving the exercise of ARCO rights.

- The Hospital centre (or medical institution). This is any private or public entity or site or medical or dental agency where clinical studies are conducted. The Centre is responsible for the Clinical Investigational File (CIF) and as such, should, among

[5] A SOP, standard operating procedure, is made up of detailed written instructions to achieve uniformity in the performance of a specific function.

other things, notify the creation of the CIF to the Spanish Personal Data Protection Agency (AEPD) prior to its creation.

The structure of the centres' personal data files takes into account the purpose for which the data are processed. Therefore a single Clinical Investigational File will be declared, which, from a conceptual viewpoint, will include the data of the subjects participating in all the studies conducted at that centre. This file will be called the Clinical research "File" (CIF). When dealing with a multicentre study, each centre where the clinical trial is conducted should declare a Clinical Investigational File

- The Investigator. This is the physician or person who exercises a profession recognised to conduct research thanks to his scientific training and requisite healthcare experience. The investigator is responsible for the completion of the clinical trial at the site and is fully integrated in its organisation. The investigator will therefore be responsible for actually fulfilling a significant part of the obligations stipulated in this Action Protocol for the party responsible for the CIF, namely, the Centre. His responsibilities include the following:

  - Agreeing and signing the study protocol together with the sponsor.
  - Having a detailed understanding of the properties of the investigational medicinal product for human use.
  - Providing information on the study to the study subjects who may request it.
  - Ensuring that informed consent is obtained in accordance with current legislation.
  - Collecting, recording and reporting data correctly and ensuring its accuracy.
  - Immediately reporting any serious adverse events to the sponsor.
  - Ensuring that all persons involved keep all information on the trial subjects confidential and ensure the protection of personal data.
  - Regularly reporting to the CEIC on the progress of the study.
  - Taking joint responsibility with the sponsor for preparing the final study report.
  - Additionally, the investigator may be asked by the Centre to fulfil any other obligation relating to data protection that may be necessary to ensure regulatory compliance.

- Subinvestigator. He forms part of the investigator's team together with his collaborators. His main functions are as follows:

  - Data entry on the CRFs.
  - Deciding on requests for information.
  - Updating the investigator's file.
  - Scheduling patients' visits during clinical trials.
  - Preparing and sending samples to central or local laboratories.
  - Accountability for returned medicinal product.
  - Arranging monitor's visits.

The Subinvestigator is normally a physician at the Centre or personnel hired through a CRO. In such cases, all references to the Centre or CRO in this Protocol will be taken into consideration.

Alternatively, when the Subinvestigator's does not form part of the Centre's organisation or has not been hired through a CRO, he will be regarded as the person responsible for processing in relation to the CIF.

- **The Contract Research Organisation (CRO).** The CRO is any individual or legal entity hired by the sponsor to carry out sponsor trial related duties.

  If the study is monitored by a CRO professional, the entity in question will be regarded as the party responsible for processing in relation to the Centre.

  Conversely, if the CRO only has access on account of the sponsor to dissociated data in order to only carry out statistical processing, he will not be accessing personal data and therefore he cannot be considered responsible for the file or processing or in charge of processing.

- **The Monitor.** The monitor is that qualified professional with the necessary clinical competence, chosen by the sponsor, who is responsible for the direct monitoring of the study. He acts as a link between the sponsor and principal investigator when they are not the same person.

  One of the monitor's main functions at the Centre where the research is conducted is to verify the accuracy and completeness of the information contained in the CRFs with respect to the source documents that form part of the subject's clinical record (tests, complementary tests, data on treatments, symptoms, signs etc).

  The monitor will perform several visits to the study site and specifically the following:

  - Pre-study visit. Checking the feasibility of the conduct of the clinical study by examining the facilities, interviewing personnel and any other checks that may be appropriate.
  - Monitoring visits. Carrying out verification functions and liaising between the investigator and sponsor. Similarly, he should check that informed consent has been correctly given by patients. In addition, he will have access to patients' clinical records to verify the accuracy of the data reflected in the CRF which will be verified "in situ" at the sites where the trial is conducted.
  - Close down visit. The monitor should prepare a final monitoring report at the closing of a site as part of the completion of the study, documenting that all the required activities to complete the study have been undertaken and that the essential documentation is stored in appropriate archives.

  The monitor accesses the personal data of the study subjects on account of the agent responsible for the file in order to provide a monitoring service. In other words, he is not involved in the decision concerning the purpose, content and use of the processing of trial subject data. Therefore the monitor will be considered in charge of the processing of the CIF.

During his visits, the monitor will confine himself to viewing the personal data accessed during his checks. Under no circumstances will he record or compile them.

In order to increase assurances concerning the dissociation procedure, the sponsor undertakes not to dismiss or penalise the internal monitor on the grounds of his refusal to disclose the subject's personal data. With respect to the external monitor, he may not terminate the contract entered into with said monitor or the CRO to which he belongs on these same grounds.

- **The Clinical Research Ethics Committee (CEIC)** in addition to the prior control of the protocol, its function is to assess and oversee the study. Access to personal data by the CEIC should not be subject to personal data protection obligations.

- **The Spanish Agency of Medicinal Products and Medical Devices** and other competent healthcare authorities may carry out various inspections *in situ* in order to check compliance with legislation and the Guideline for Good Clinical Practice and issue a report, without identification details, which will be made available to the parties inspected and the European Medicines Agency.

- **The Auditor.** The auditor is any individual or legal entity responsible for the independent and systematic examination of the activities and documents related to the study in order to determine whether the activities evaluated in connection with the study were conducted and the data were correctly recorded, analysed and reported in accordance with the protocol, Standard Operating Procedures (SOP), the Guideline for Good Clinical Practice and regulatory requirements.

  If the auditor's involvement is required, he will access the personal data of the study subjects on account of the Centre manager in order to provide audit services. In other words, he is in no way involved in the decision concerning the purpose, content and use of the processing of the study subjects' data. Therefore the auditor will be considered responsible for the processing of the CIF.

  The auditor will confine himself to viewing the identification data accessed during his verification and will not register or record them on any carrier media under any circumstances.

  The internal auditor may not be dismissed or penalised for refusing to disclose the subject's identification details. With respect to the external auditor, the contract between the external auditor and sponsor may not be terminated by the sponsor for this same reason.

Set out below is a summary of the position which, from the point of view of personal data protection, is held by each of the parties involved in a study with dissociated data in relation to the CIF.

LOPD	Centre	Sponsor	Monitor	Auditor	Subinvestigator
Responsible for the Clinical Investigational File	X				
Responsible for processing Clinical Research		X			
In charge of processing			X	X	X

As mentioned earlier in this Protocol, the Centre, as the party responsible for the Clinical Investigational File should declare it prior to its creation. **Annex III** sets out, for guidance, the typical structure of a CIF which should be adapted on the basis of the research conducted at each centre.

Moreover, if a CRO is providing services other than monitoring services, i.e. work associated with the sponsor, and on the basis that he does not have access to any personal data and nor does he have any decision-making power in relation to the relevant processing criteria, he would not hold any legal position with respect to the CIF from a data protection viewpoint.

Lastly and as was indicated at the outset, the sponsors and CROs adhering to the Standard Code will ensure that the other parties involved in a Clinical research collaborate with them in fulfilling the obligations of this Action Protocol.

The active collaboration of the investigators, monitors, auditors and all their collaborators will therefore be requested in order to cooperate with the sponsors and CROs adhering to the Standard Code in fulfilling their obligations and keeping the data accessed confidential in accordance with current legislation and at all times subject to the duty of secrecy inherent in their profession.

Therefore, and irrespective of the agreements that each of the parties involved in the Clinical research should enter into, all of them should sign a Confidentiality Agreement with the Centre responsible for the CIF the content of which should be similar to that included in **Annex IV**.

3. Dissociation procedure.

Personal data cannot be considered a determinant factor for the conduct of the study and are therefore systematically dissociated, the information being held solely by the investigator. It is very important to bear in mind that when the sponsor opts to obtain dissociated data, it is precisely because he does not want to have the personal data of the study subjects although he should verify through the monitor and in order to ensure the study's validity, that the results obtained are not fictitious and derive from real subjects.

Once consent has been obtained from the participating subjects and as one of the key tools in any clinical study, the investigator completes a CRF for each study subject.

In accordance with the definition contained in the Guideline for Good Clinical Practice (CPMP/ICH/135/95), a CRF is a printed, optical or electronic document designed to collect and transmit to the sponsor all the information required under the protocol on each study subject.

Therefore the CRFs used in practice may be on paper or in an electronic format. The basic difference will be the manner in which they are accessed by the parties involved in the study.

CRFs on paper may be consulted "in situ" by the monitor. They will be sent to the sponsor, where appropriate, and at all times following the dissociation guidelines described below and a copy will be left at the centre in accordance with the Guideline for Good Clinical Practice. Access to or the enquiry of electronic CRFs is remote by each

of the parties involved in the clinical study through their respective computers. The monitor and sponsor are therefore able to access the CRFs in real time.

CRFs should be in a format that helps to complete them with the least risk of error possible. They should therefore contain the necessary explanations concerning any fields that may trigger doubts. As far as possible, reference should be made to the options and numerical ranges applicable to the data to be collected. For electronic CRFs, systems should be applied to prevent errors, discrepancies and inconsistencies in the introduction of data. The professionals responsible for completing the CRFs should receive the necessary information to ensure that they are completed as accurately as possible. These CRFs will contain the fields strictly necessary to attain the objectives of the research project to which they relate.

The content of the CRF, which is to be completed by the investigator, will relate to the clinical information contained in the subject's clinical records and the information generated in the course of the study[6].

The investigator is responsible for carrying out the dissociation procedure. On observational studies, a numerical or alphanumerical code will be assigned in strict consecutive order to each subject. This will be provided by the sponsor and bear no relation to the participating subjects' identification details.

On clinical trials, each subject will be assigned a numerical or alphanumerical code on a random basis which is usually generated by a bio-statistician using a computer program with a standard procedure to generate random numbers. For example, on multi-centre trials, once a patient's eligibility has been confirmed, the investigator contacts the randomization centre to obtain the patient's randomization number and the treatment assigned. If a patient withdraws from the trial, his study patient number cannot be reused. Moreover, the monitor should verify that the dissociation process has been correctly completed and the data provided to the sponsor do not contain the subject's identification details.

The investigator should reflect each code in the pertinent CRF, without including any other identification details to ensure that the sponsor is unable to identify the study subject when he receives the CRFs. This will enable he subject’s identification details to be dissociated from the rest of the information obtained during a Clinical research.

The list of identification data and dissociation codes relating to the study subjects is safeguarded by the investigator at the centre where that study is undertaken such that it is guaranteed that no other agent involved in the study, except for the monitor, the auditor and the inspector, has access to the aforementioned list. Similarly, those responsible for ensuring the dissociation will undertake to at all times act following their own criteria during the performance of their work and not accept any type of instruction or suggestion that may alter the complete dissociation of the subject’s identity from the other information obtained during the research. Moreover, they should at all times maintain the identification data that they may access secret, fulfil the obligations contained in the LOPD and enabling regulations and observe the instructions that, in relation to information security, are reported to it by the sponsor, investigator and centre where the research is conducted.

[6] A clinical record is the set of documents containing the clinical data, assessments and evolution of a patient over his medical history.

4. Adverse events.

An adverse event is any untoward medical occurrence in a Clinical research subject to whom a medicinal product is administered although there may not necessarily be a causal relationship with this treatment.

Clinical trials

a) The investigator will report the sponsor immediately of any serious adverse effects, according to the requirements and procedures laid down in the protocol. Subsequently the investigator should provide the sponsor with the details related to the adverse event detected.

   For its part, the sponsor should keep detailed records of all the adverse effects reported to it by the investigator and that should be submitted to the AEMPS upon request.

   If the adverse event relates to or results in the death of a trial subject, the investigator should provide the sponsor with all the complementary information required such as for example, autopsy reports, after having previously concealed all the subject's identification data.

   All the notifications referred to above will identify the subject affected by the adverse event through an identification code such that the sponsor does not have access to the trial subject's identification data.

b) In the event of serious unexpected adverse reactions, the sponsor will be responsible for reporting them, within the legal periods, to the AEMPS, competent bodies of the Autonomous Regions and Clinical research Ethics Committees. Moreover, annual safety reports and "ad hoc" reports should be prepared in the event of major safety concerns. Communications between the sponsor and these entities will not include the trial subjects' identification data.

   It is the sponsor's responsibility to adequately indemnify the subjects except in the event of negligence on the part of the parties involved. In order to address this type of unexpected situations, the sponsor will be required to arrange before the initiation of a clinical trial, insurance or an equivalent financial guarantee, except in low risk trials with medicinal products that have already been approved and are used under authorised conditions.

   The investigator will be responsible for transferring the data of the subjects involved to the insurance company for it to have the necessary information to provide the coverage arranged. In this case, the insurance company will be responsible for its own file with respect to the information provided to cover the claim.

Observational studies

There may be adverse reactions on observational studies. An adverse reaction to a medicinal product is any noxious unintended response related to the medicinal product irrespective of the dose. The expression "response to a medicinal product" means that

there is a reasonable possibility that there is a cause and effect relationship between the adverse event and the medicinal product.

- The investigator will immediately notify the sponsor of any serious adverse reactions, in accordance with the requirements and procedures contained in the protocol. The investigator should subsequently provide the sponsor with new details related to the adverse reaction detected.
- The sponsor will report to the autonomous region where the investigator works any serious adverse reactions notified during the study[7].
- On observational studies, it is not mandatory to arrange insurance or a financial guarantee since the medicinal products are used under habitual conditions of use as specified in their Summary of Product Characteristics.

5. Termination of the study.

Once the study has been completed, as envisaged in the protocol, the sponsor will receive from the investigator the information and conclusions without personal details and will report them to the health authorities. The documentation generated as a result of the Clinical research will remain in the centre, irrespective of the investigator's destination upon the termination of the study.

The essential documentation on the clinical trial will be kept for the periods that figure below in the centre's and sponsor's archives, as appropriate for each type of documentation:

- The sponsor and investigator will keep the essential documents on each clinical trial for at least 5 years following the termination of the trial or for longer if so required, as in the case that the study is submitted as a basis to register a medicinal product which should fulfil the conditions of Annex I of Royal Decree 1345/2007, of 11 October 2007, or an agreement is entered into between the sponsor, the investigator and the centre.
- Marketing authorization holders should adopt the necessary measures to ensure that the essential clinical trial documents (including case report forms) other than the subject's Clinical file are safeguarded by the data owners:[8]
  - A minimum of 15 days following the study's interruption or termination; or
  - A minimum of 2 years from the last time marketing authorisation was granted by the European Union and in those cases where there are no marketing applications pending or planned in the European Union; or
  - A minimum of 2 years following the official interruption of the clinical development of the investigational product.

Similarly, and irrespective of the duration of storage, the documentation should be filed in such a way that it may be easily made available to the regulatory authorities upon request.

[7] Royal Decree 1344/2007, of 11 October 2007, on pharmacovigilance of medicinal products for human use.

[8] Royal Decree 1345/2007, of 11 October 2007 establishing the procedure for authorising and registering and laying down the conditions for supplying industrially manufactured medicinal products for human use.

Specifically, signed informed consent forms, the subject's source medical records, the list of subject identification codes and the subject inclusion register should be filed at the centre.[9]

The sponsor may decide to terminate the trial early and the authorities may suspend or revoke the authorisation to carry it out, provided that the conditions laid down in Royal Decree 223/2004, of 6 February 2004, governing clinical trials with medicinal products are met. In any event and as in the case of the ordinary termination of the trial, all communications and files resulting from the performance of the trial should exclude the identification details of the subjects participating in that clinical trial.

6. Access to data by third parties.

The Sponsors who have applied the dissociation procedure contained in this section may freely report the dissociated data to other individuals and legal entities.

7. Safety measures.

The Sponsors who have applied the dissociation procedure described above will not be required to apply security measures to dissociated data.

8. International transmissions

The Sponsors who have applied the dissociation procedure contained in this section may freely report dissociated data to other individuals or legal entities, irrespective of the home country where they are based.

9. Access, rectification, cancellation and opposition rights (ARCO).

As a result of the application of the aforementioned dissociation procedure, the sponsor will not have the personal data of the trial subjects and will therefore be unable to address requests for the exercise of ARCO rights.

Nonetheless, the sponsors are required to reply to the request addressed to them, irrespective of whether or not they include the subject's personal data.

In order to exercise ARCO rights, the sponsor should act in accordance with the Action Protocol on ARCO rights.

[9] CPMP/ICH 135/95 Guideline for Good Clinical Practice.

IV. CLINICAL RESEARCH USING PERSONAL DATA.

1. Introduction.

As mentioned in previous sections of this Protocol, in certain clinical trials, the sponsor may decide, owing to company policy, to access the personal data of the subjects participating in a Clinical research.

Similarly, there is another series of very limited and exceptional instances where the sponsors that sponsor Clinical research using dissociated data may access the subjects' identification data.

Although the probability of such instances arising is minimal, on the basis of a theoretical analysis, it is possible to identify the following exceptions:

- Spontaneous contact of the subject with the sponsor.
- Damages to the subject requiring economic compensation.
- Human error.
- Any other exceptional circumstances beyond the sponsor's control which in any way enable the subject's identity to become known.

Sponsors will apply the relevant measures to avoid such instances. The following are particularly noteworthy.

- Written instructions addressed to the subject, included in the informed consent, as to how to contact the investigator on any matter related to the study.
- Processing of compensation for damages through the insurance company.
- Standard Operating procedure aimed at the prevention of human error.
- Personal data filter system.

If, despite the application of such preventive measures, the sponsor identifies the subject, the sponsor could choose between the following:

- Applying high level security measures to the file and fulfilling the requirements of the LOPD and enabling regulations.
- Creating a specific high- level file on a computer which is separate from the system containing the data of the subjects whose identification data have become known to the laboratory.
- Cancelling the affected subject's identification details.

On studies involving personal data, high- level security measures will be applied to the file, the requirements of the LOPD and RLOPD will be met and no dissociation procedure will be carried out. Therefore communications between the investigator and the sponsor, directly or through the monitor, will include the personal data of the subjects involved in the Clinical research.

In particular, the CRFs will be sent to the sponsor after including in them the trial subjects' personal data.

The development and termination of Clinical research using personal data are similar to the section on Clinical research using dissociated data, with the obvious specific features deriving from the processing of personal data by the sponsor.

2. Management and Conduct of the Study

Once consent has been obtained from the participating subjects in accordance with the section "Initiation of a Clinical research" and as a key tool on any clinical study, the investigators will complete a CRF for each trial subject.

Following the protocol's instructions, the investigator and his collaborators will carry out the necessary actions and include the clinical information generated in the course of the study in the CRF on each subject. The investigator, as the party ultimately responsible for completing the CRF, should sign such documents.

In the course of the study, various agents will contact the investigator who will be required to permit and facilitate the oversight, audit and inspection work.

Set out below is a list of such agents, their main responsibilities and legal position in relation to trial subjects' personal data.

- **Sponsor.** His responsibilities are the same as those already mentioned in the section on Clinical research using dissociated data and in this case. The sponsor may establish direct communication with the investigator with no need to ensure that data which may identify the study subject are excluded. Nonetheless, access to subjects' personal data will be limited to that strictly necessary for the correct conduct of the study.

  The sponsor will in turn be required to declare a Case Report Form (CRF), the content of which is set out in **Annex V** of this protocol.

- **The hospital centre (or healthcare institution).** As has already been mentioned, the hospital centre or healthcare institution will be that private or public medical or dental entity or site or agency where the clinical studies are conducted.

  The Centre will in turn be required to declare a Clinical Investigational File (CIF).

- **The Investigator.** The investigator is responsible for the conduct of the clinical trial at a centre and his responsibilities include those already mentioned for the Clinical research using dissociated data. The investigator is responsible for the performance of the clinical trial at a centre and is fully integrated in its organisation. The Investigator will therefore be responsible for actually fulfilling a significant portion of the obligations stipulated in this Action Protocol for the person responsible for the CIF, i.e. the Centre (see section on "Clinical research using dissociated data").

- **The <u>Subinvestigator.</u>** The subinvestigator is part of the investigator team and carries out investigator support duties (see section on Clinical research using dissociated data").

The subinvestigator is normally a physician of the Centre or personnel hired through a CRO. In such cases, the provisions applicable to the Centre or CRO under this Action Protocol will be applicable, respectively.

Conversely, when the subinvestigator is not integrated in the Centre's organisation or has not been hired through a CRO, he will be considered responsible for the processing in relation to the CIF.

- **The CRO.** The CRO is any individual or legal entity hired by the sponsor to carry out the sponsor's functions or duties. If he carries out functions related to the monitoring of the study, he will be considered responsible for the processing of the CIF, for which the Centre is responsible. Conversely, if he carries out the processing of data included in the file which is the sponsor's responsibility, on account of the sponsor, he will be responsible for processing the CRFF. Therefore and as a summary:

  - The CRO is hired for monitoring tasks: Responsible for processing in relation to the Clinical Investigational File.
  - The CRO is hired by the sponsor to carry out tasks other than monitoring tasks: Responsible for processing in relation to the CRFF.

- **The monitor.** The monitor is the link between the sponsor and principal investigator and carries out direct monitoring tasks in relation to the study. He has exactly the same functions and obligations as contained in the section on Clinical research using dissociated data and makes the same mandatory visits as already mentioned. The monitor is regarded as the person responsible for processing in relation to the CIF.

  It should be borne in mind that the only reason why the monitor has access to the CIF is to verify that the data included in the CRF are indeed those resulting from the Research.

  In short, the monitor accesses the CIF to verify that the assignment of the Centre's data to the Sponsor, establised in the contract between both, has been correctly completed and therefore should assume a special duty of confidentiality and secrecy in relation to the data accessed to carry out his functions (see **Annex IV**).

- **The Clinical Research Ethics Committee (CEIC).** As has been described in the section on Clinical research using dissociated data, the CEIC does not have any responsibility for the file and is not responsible for its processing.

- **The Spanish Agency of Medicines and Medical Devices.** As is set out in the section on Clinical research using dissociated data, these authorities should be considered responsible for their own files with respect to the inspections conducted by them.

- **The Auditor.** As in the case of a Clinical research using dissociated data, the auditor is considered responsible for processing in relation to the CIF.

  It should be borne in mind that the only reason why the auditor has access to the CIF is to verify that the data reflected in the CRF are indeed those resulting from the research.

In short, the auditor accesses the CIF solely to verify that the assignment of the Centre's data to the Sponsor, provided in the contract between both, has been correctly completed and therefore he should take on a special duty of confidentiality and secrecy in relation to the data to which he may have access to carry out his duties.

As a summary, set out below are two tables that sum up the positions that from the point of view of personal data protection, are held by each of the parties involved in a study with personal data in relation to the CIF and CRFF.

Clinical Investigational File (CIF)

As the Centre will be collecting personal data on the subjects participating in the study, it will be required to declare a Clinical Investigational File to the AEPD Registry prior to its creation.

In relation to the CIF and although the Sponsor only accesses the data that are contained in the Case Report Form, said Sponsor is responsible for deciding, inter alia, the criteria that determine the subject's participation in the trial, informing the healthcare authorities, providing the guidelines on preparing the mandatory reports etc.

In short, the sponsor establishes guidance for processing the personal data of the trial subjects. This means that the Sponsor is responsible for processing in relation to the CIF while the Centre is responsible for the CIF.

The structure of the centre's personal data files conforms to the purpose for which the data are collected. Therefore a single Clinical Investigational File will be declared that will include the details of the subjects participating in all the studies being conducted at that centre. This file will be named the "Clinical Investigational File" (hereinafter the CIF). In the event that we are dealing with a multicentre study, each centre where the clinical study is conducted should declare a CIF.

Annex III sets out, for guidance, the typical structure of a CIF which should be tailored on the basis of the type of Clinical research conducted by the centre.

In relation to this file, the parties involved who would be able to access the data and the positions that they hold in relation to data protection are set out in the table below:

LOPD	Centre	Sponsor	Monitor	Auditor	Subinvestigator
Responsible for the file	X				
Responsible for processing		X			
In charge of processing			X	X	X

Case Report Form File (CRFFs)

Apart from the content of the CRFs, the sponsor does not have access to any other documentation recording the subjects' personal data.

In contrast to Clinical research using dissociated data, the CRFs accessed by the sponsor include trial subjects' personal data. In this case, the sponsor acts as the

person responsible for the file and decides on the purpose, content and use of the data contained in such CRFs and is in turn responsible for the processing of the CRFF. Therefore, the sponsor, as the person responsible for the file, should declare a CRFF prior to its creation.

In particular, the purpose of the CRFF consists of assessing the results of the study and drawing up the conclusions and final reports, as appropriate, that will exclude any personal data.

It should therefore be noted that the CRFF for which the sponsor is responsible does not coincide in terms of content or purpose with the CIF, for which the Centre is responsible, and they should therefore be arranged as two different files.

Nonetheless, the Centre carries out the assignment of certain data to the sponsor. Such data relate solely to the identification details of the subjects participating in a Clinical research who figure in the CRF. In this respect, the contract between the Centre and the sponsor should provide the pertinent guarantees in relation to personal data protection for the assignment of data.

The structure of the centre's personal data files conforms to the purpose for which the data are processed and therefore a single CRFF will be declared that will comprise the data of the subjects participating in all the studies sponsored.. This file will be named the "Case Report Forms File" (CRFF). **Annex V** sets out, for guidance, the typical structure of a CRFF which should be tailored on the basis of the type of Clinical research conducted by the sponsor.

Lastly, the CROs, when not carrying out monitoring work, will be considered in charge of processing on behalf of the sponsor with respect to the CRFF.

In relation to this file, the parties who would be able to access the data and positions which they hold in relation to data protection are set out in the following table:

LOPD	Sponsor	CRO (work other than monitoring)
Responsible for the file	X	
Responsible for processing	X	
In charge of processing		X

Lastly, and as was explained at the start of this action protocol, the sponsors and CROs adhering to the Standard Code will ensure that the other parties involved in a Clinical research collaborate with them in complying with the obligations contained in this Action Protocol.

In this way, the active collaboration of the investigators, hospital sites, monitors, auditors and all their collaborators will be required to ensure cooperation with the sponsors and CRO adhering to the Standard Code in fulfilling their obligations, keeping the data they access confidential in compliance with current legislation and at all times in accordance with the duty to secrecy inherent in their profession.

Therefore and irrespective of the agreements that should be entered into with each of the parties involved in a Clinical research, all of them should enter into a Confidentiality Agreement with the Centre responsible for the CIF, the content of which should be similar to that included in **Annex IV**.

3.- Adverse events.

Both the procedure and obligations of the parties in relation to adverse events are the same as those indicated for Clinical research using dissociated data. However, there is no need in this case for the investigator's communications to the sponsor to exclude identification data although such data should be excluded in the communications between the sponsor and the authorities (AEMPS, competent bodies of the Autonomous Regions) and the CEIC.

The investigator or sponsor himself may be in charge of transferring the data of the affected subjects to the insurance for it to have the necessary information to provide the coverage arranged. As in a Clinical research using dissociated data, the insurance company will be responsible for processing with respect to the information provided as a result of the claim filed.

4.- Termination of the study.

Following completion of the study, in accordance with the protocol, the sponsor will receive from the investigator the information and conclusions of the same, including the personal data contained in the CRF which will form part of the CRFF. The documentation generated in the centre as a result of the Clinical research will remain in the centre, irrespective of the investigator's destination upon completion of the study.

The essential documentation concerning the clinical trial will be stored for the periods that figure below in the centre's or sponsor's archives, as appropriate for each type of documentation:

- The sponsor and the Centre: will keep the essential documents for each clinical trial for at least 5 years following completion of the trial or for a longer period if thus established by other applicable requirements, as in the event that the study is presented as a basis for registering a medicinal product with respect to which Annex I of Royal Decree 1345/2007 (11 October) should be observed or there is an agreement between the sponsor, the investigator and the centre.[10]

- The laboratory sponsoring the study should take the necessary measures to ensure that the essential documents concerning the clinical trials (including the case report forms) and other than the subject's medical files are safeguarded:[11]
  - A minimum of 15 years following the interruption or completion of the study; or
  - A minimum of 2 years from the date of the last marketing authorisation from the European Union and where there are no marketing applications pending or planned in the European Union; or
  - A minimum of 2 years following the official interruption of the clinical development of the investigational product.

[10] Order SCO/256/2007 of 5 February 2007 laying down the principles and detailed guidelines for Good Clinical Practice and the requirements to authorise the manufacture or import of investigational medicinal products for human use.

[11] Royal Decree 1345/2007 of 11 October 2007 regulating the procedure for the authorisation, registration and the conditions for supplying industrially manufactured medicinal products for human use.

Similarly, and irrespective of the storage time, documentation should be filed in such a way that it may be easily made available to the regulatory authorities upon request.

Specifically, the signed informed consent forms, the source documents of the subject's records, the list of subject identification codes and the subject inclusion record will be stored in the centre's archives.[12]

Moreover, the sponsor may decide to bring the trial to an end early and the authorities may suspend or revoke the authorisation to conduct it, provided that the conditions contained in Royal Decree 223/2004 of 6 February 2004 governing clinical trials with medicinal products are met.

5.- Third-party access to data.

5.1. Party in charge of processing.

Occasionally there may be third parties accessing the personal data of the subjects participating in clinical trials because they provide a service. For Clinical research, such service providers are normally the CROs.

If there is a service provided in the terms indicated above, a contract should be executed between the Centre and the provider, considered as the person in charge of the processing, stipulating that the latter will only process the data in accordance with the sponsor's instructions, that he will not apply or use them for any purpose other than that which figures in that contract, and will not disclose them, not even for storage, to other persons.
The contract will similarly stipulate the security measures applicable to the data accessed and that the provider is required to implement.

Once the service under the contract has been completed, the personal data should be destroyed and/or returned to the person responsible for processing together with any carrier media or documents containing any personal data subject to processing.

In the event that the provider, as the party in charge of processing, uses the data for other purposes, reports them or uses them in breach of the contract, he will also be considered responsible for processing and will be liable for any violations committed on a personal basis.

Annex VI to this Protocol includes the standard clause that should be signed between the party responsible for the file and those providers with access to personal data.

5.2. Reporting to other group companies or third companies

The reporting of personal data to other group companies or third companies will call for the unequivocal and individual consent of the affected party to the assignment of his data to group companies. The list of companies may be easily identified and consulted by the affected party (eg. a webpage) or consent may be secured to report personal data to pharmaceutical companies of the same business group or third companies and for the same purpose in relation to the processing of personal data.

[12] CPMP/ICH/135/95 Guideline for Good Clinical Practice.

5.3. Reporting to the parent company.

Reporting personal data to the parent company will require the unequivocal consent of the affected party. Consent should take into account whether the company is located in a country with protection comparable to that in Spain.

If the parent company is notified under a services contract and it is located in the European Economic Area, the regime pertaining to processing engagements will be applied, as provided in section 5.1 of this Action Protocol.

If the information reported to the parent company is not personal because it is dissociated data, involves aggregate or statistical data or any other data which, by law, is not considered to include personal data, the provisions contained in this paragraph and in paragraphs 5.2., 5.4 and 5.5, will not apply.

5.4. Communication provided by Law.

There will be no need for the consent of the affected party to reporting data to the national or international healthcare authorities in accordance with applicable Clinical research legislation.

Nor will consent be required when there is an assignment of personal data concerning health necessary to either solve an emergency that requires accessing a file or to conduct epidemiological studies in the terms contained in central or regional government healthcare legislation.

6.- Security measures.

The sponsor should apply high level security measures to the CRFF, taking into account the specially protected character of the health data reported. In this respect, the sponsor will have a security document that will contain the technical and organisational measures that all persons with access to the personal data contained in the CRFF will have to observe, in accordance with Article 88 of the RLOPD. This document will set out all the security measures that are applicable in accordance with Title VIII of such regulations.

7.- International transmissions.

An international transmission of data is all processing of data that entails transferring data outside the European Economic Area whether it is arranged as an assignment or reporting of data or is aimed at the processing of data on account of the person responsible for the file established in Spanish territory.

Instances in which an international transmission could be required.

The instances in which the Sponsors carry out international transmission of data of study subjects involve communications which, in accordance with applicable internal policies, should be made to the parent companies located outside the European Economic Area for the purposes of the analysis and follow-up of the study and its control.

Information on subjects who have given their consent to participate in the study will be reported. The Sponsors should observe the considerations and guidelines set out below, taking into account the country where the parent company is located.

Of the international transmissions to be made, those to States providing an appropriate level of security should be differentiated from those not affording a level of protection comparable to that under Spanish legislation.

a) States providing an adequate level of protection

Those States which the European Commission, through its reports, or the Spanish Data Protection Agency, through its resolutions published in the Official State Journal, has declared, ensure an adequate level of protection are considered to afford an appropriate level of protection.

Similarly, this group of States providing an appropriate level of protection should include those US entities adhering to the so-called *Safe Harbour Agreement*. This Agreement derives from the need to bring Community data protection legislation closer to the operation of US companies where there is a different approach to data protection compared with Europe.

For this reason, in 2000 the European Commission approved the aforementioned Agreement, drawn up by the US Commerce Department, in accordance with it, those companies and entities adhering to the Agreement will be understood to afford protection comparable to that under Community legislation such that data flows will be permitted between these and other entities of EU Member States.
In the event that the destination of the international transmission is a country with an adequate level, the Data Protection Registry will only need to be informed.

The updated list of countries offering a comparable level of data protection may be consulted on the AEPD web page (www.agpd.es).

b) States that do not provide an adequate level of protection

The transfer of data to countries with an inadequate level of protection should be authorised previously by the Agency's Director. Such authorisation will be granted following the procedure contained in the RLOPD (Articles 137 to 144).

The laboratories may, however, transmit data to countries not providing an adequate level of protection with no prior authorisation of the Agency's Director provided that the international data transfer conforms to any of the following:

- Transmissions resulting from the application of Treaties or Conventions to which Spain is party.
- For reasons of international legal or health (healthcare and prevention) assistance or for the recognition, exercise or defence of rights during a legal process.
- At the request of both a subject with a legitimate interest and a Public Registry and in accordance with the purpose of such interest.
- Prior and unequivocal consent of the affected party to the transmission. Generally speaking, the subject's prior and unequivocal consent through the use of the clause contained in Annex **I and II**, in particular, informing him, moreover, of the fact that:

His personal data may also be stored by group companies at international level and by companies for the performance, inter alia, of the statistical analysis of the study conducted. He may consult the group companies to which his data will be assigned and the countries where such countries are located on the laboratory's web page".

If the subject's consent has not been obtained in accordance with the aforementioned clause, the authorisation of the AEPD's Director will be required for the international transfer of the healthcare professional's data to States that do not afford an adequate level of protection.

In this case, the obligation to notify and register the international transfer with the Data Protection Registry should also be complied with.

c) *Corporate Binding Rules*

International data transmissions to States that do not provide an adequate level of protection include specifically data transmissions between companies located in different States but that are part of the same multinational group.

In such cases, the Agency's Director may authorise those international transmissions that take place within a multinational group of companies provided that such group has adopted a series of internal rules or regulations binding on all group companies ensuring compliance with the principles and exercise of the rights recognised under the LOPD.

8.- Rights of Access, Rectification, Cancellation and Opposition (ARCO).

The subjects involved in a clinical research may exercise access, rectification, cancellation and opposition rights. The pertinent requests will be addressed through the Action Protocol on ARCO rights.

Annex I[1]

(Minimum content on data protection to be included in informed consent on a Clinical research using personal data processed exclusively by the Centre - Clinical research using dissociated data)

"In accordance with current data protection legislation, you expressly consent to having data from your clinical records and those resulting from your participation in the study included in a personal data file under the Centre's responsibility.

Access to personal information will be restricted to the study's physician and his collaborators, healthcare authorities, Clinical Research Ethics Committee and the sponsor's monitors and auditors, who will be subject to the duty of secrecy inherent in their profession, when access is required to verify the data and procedures of the study, but at all times, ensuring confidentiality in accordance with current legislation.

Lastly, you may exercise the rights of access, rectification, cancellation and opposition in relation to data for which you should contact the Centre where the study was conducted: (Centre name and address, etc)

[1] *The content of this Annex will be fulfilled nn a case by case basis.*

ANNEX II[2]

(Minimum content on data protection to be included in informed consent on Clinical research using personal data received / processed by the laboratories promoting Clinical research)

"In accordance with current data protection legislation, you expressly consent to having data from your clinical records and those resulting from your participation in the study included in two personal data files under the responsibility of the Centre and the sponsor of the study, respectively, the sponsor adhering to the Standard Code on Clinical Research and Pharmacovigilance of Farmaindustria, and which may be consulted.

The recipients of the personal data contained in the files for which the Centre and Sponsor are responsible will be the following:

1. *The medical centre / hospital where the patient is attended to, that will introduce the data in a file, duly reported to the Spanish Data Protection Agency.*
2. *The physician that attends to him, who will introduce the data in the medical centre or hospital file.*
3. *The parent company of the laboratory sponsoring the study, that coordinates the research internationally and files the results at its headquarters in (…City and Country …) [Legal notice: section 3 will only be applicable where data is to be provided to the parent of the laboratory sponsoring the study].*

Similarly, there may be other parties who access data when required to check the data and procedures of the study, although at all times ensuring confidentiality in accordance with current legislation (such parties are the monitor, the auditor, the healthcare authorities, the Clinical Research Ethics Committee).

If you wish to exercise your rights of access, rectification, cancellation and objection, you should visit the following addresses (complete, as appropriate, with the identification data of each of the files created and its address):

1. *For the file for which the Centre is responsible, the request should be addressed to: (…Centre name and address …).*
2. *For the file for which the laboratory sponsoring the study is responsible, the request should be addressed to: (..Laboratory name and address).*

In order to exercise such rights, you can find a standard request in the Farmaindustria Standard Code".

[2] *The content of this Annex will be fulfilled On a case by case basis.*

ANNEX III[3]

Clinical Investigational File (CIF)

1.- Information concerning the party responsible for the CIF.

- Company name.
- Tax ID.
- Registered office.
- Location.
- Post code.
- Province.
- Country.
- Telephone.
- Fax.
- Email.

2.- ARCO rights.

In the event that the address indicated for the affected parties to exercise their ARCO rights differs from that of the party responsible for the CIF, this should be indicated.

3.- Party in charge of processing.

If there is a third party providing services to the party responsible for the File that, as a result of that provision of services, accesses CIF data, the CIF should reflect the following information in relation to the party in charge of processing:

- Company name.
- Tax ID.
- Postal address.
- Location.
- Post code.
- Province.
- Country.
- Telephone.
- Fax.
- Email.

If there are various parties in charge of processing and not all of them can be duly reflected, the party that will provide the services over the longest period of time or that which entails the greatest risks because of the type and quantity of data processed should be reflected.

All the information contained in this section should be understood without prejudice to the fact that an agreement on data protection should be entered into between the party responsible for the file and the party in charge of processing in the terms of Article 12 of LOPD and 20 et seqq. of the RLOPD.

4.- Identification and purpose of the CIF.

- File name. The file's name could be "Clinical Investigational File"

[3] *The content of this Annex will be fulfilled on a case by case basis.*

- Detailed description of the purpose and uses envisaged of the "Clinical Investigational File". The detailed description of the purpose of the file would agree with "The management of the study conceived in a general manner".

5.- Origin and source of data

The origin of the data will be the subject's medical record. The interested parties would mainly be patients and other subjects participating in the Clinical research.

6.- Types of data, structure and organisation of the CIF.

The data that will be collected on the participating subjects may be, inter alia, as follows:

- Health.
- Medical record.
- Medical ID.
- Images (imaging diagnosis tests).
- Name and surname.
- Tax ID/National ID.
- Address.
- Telephone.
- Physical marks.
- Signature.
- Personal characteristics.
- Social circumstances (hobbies and life style).
- Academic and professional.
- Other types of data.

7.- Processing system.

Generally speaking, the documentation generated in relation to Clinical research is processed on paper and electronically and therefore, except in exceptional cases, the processing system would be **a combination of both.**

8.- Level of security measures.

As the data processed will relate to participating subjects' health, the applicable level of security measures is **high.**

9.- Assignment or communication of data.

The bodies or entities to which the data of subjects participating in the clinical trial will or may be assigned are, at least, the following:

- Bodies or persons directly related to the party responsible.
- Insurance companies.
- Other bodies of the Public Administration.

10.- International transmission.

This section should reflect the countries and categories of the parties to which the data are assigned and that do not form part of the European Economic Area.

ANNEX IV[4]

Confidentiality agreement – Parties involved with access to personal data.

1. The agent or worker undertakes to keep the personal data of the subjects in a Clinical research to which they may have access in the performance of their tasks, in the maximum confidence and secrecy, particularly when they refer to health data. The agent or worker undertakes not to disclose such data and not to publish them or make them available to third parties directly or through third persons or companies.

2. Similarly, the agent or worker undertakes, following the termination of this contract, not to keep a copy of any documentation which may contain the personal data of the subjects in a Clinical research.

3. The agent or worker recognises that personal data protection legislation lays down a series of obligations with respect to personal data access. For such purpose, the agent or worker undertakes to access the subject's personal data, to comply with data protection legislation and the specifics of the action protocol on clinical trials and other Clinical research of Farmaindustria's standard code.

4. The obligations of confidentiality contained in this contract shall be indefinite and remain in effect after the termination of the employer/ employee or mercantile relationship between the Centre / Sponsor and the worker.

[4] *The content of this Annex will be fulfilled on a case by case basis*

ANNEX V[5]

Case Report Forms File (CRFF)

1.- Information concerning the party responsible for the CRFF

- Company name.
- Tax ID.
- Registered office.
- Location.
- Post code.
- Province.
- Country.
- Telephone.
- Fax.
- Email.

2.- ARCO rights

In the event that the address indicated for the affected parties to exercise their ARCO rights differs from that of the party responsible for the CRFF, this should be indicated.

3.- Party in charge of processing

If there is a third party providing services to the party responsible for the File that, as a result of that provision of services, accesses CRFF data, the CRFF should reflect the following information in relation to the party in charge of processing:

- Company name.
- Tax ID.
- Postal address.
- Location.
- Post code.
- Province.
- Country.
- Telephone
- Fax.
- Email.

If there are various parties in charge of processing and not all of them can be duly reflected, the party that will provide the services over the longest period of time or that which entails the greatest risks because of the type and quantity of data processed should be reflected

All the information contained in this section should be understood without prejudice to the fact that an agreement on data protection should be entered into between the party responsible for the file and the party in charge of processing in the terms of Article 12 of LOPD and 20 et seqq. of the RLOPD.

4.- Identification and purpose of the CRFF

- File name. The name of the file could be the "Case Report Form File"

[5] *The content of this Annex will be fulfilled on a case by case basis*

- Detailed description of the purpose and uses envisaged of the "Case Report Form File". The detailed description of the purpose of the file would agree with "Evaluation of results and issue of conclusions in relation to clinical trials and other Clinical research sponsored by the party responsible for the File".

5.- Origin and source of data

- The interested party itself. The interested parties would be the patients and other subjects participating in Clinical research.
- Private Entity. These private entities refer to the Centre that is not a Public Entity.
- Other groups. Public sector centres.

6.- Types of data, structure and organisation of the CRFF

The data that will be collected on the participating subjects may be, inter alia, as follows:

- Health.
- Medical record.
- Image (image diagnosis tests).
- Name and surnames.
- Tax ID/National ID.
- Address.
- Telephone.
- Physical marks.
- Signature.
- Personal characteristics.
- Social circumstances (hobbies and life style).
- Academic and professional.
- Other types of data.

7.- Processing system

Generally speaking, the documentation generated in relation to Clinical research is processed on paper and electronically and therefore, except in exceptional cases, the processing system would be **a combination of both.**

8.- Level of security measures

As the data processed will relate to participating subjects' health, the applicable level of security measures is **high.**

9.- Assignment or communication of data

The bodies or entities to which the data of subjects participating in the clinical trial will be or may be assigned are, at least, the following:

- Bodies or persons directly related to the party responsible.
- Insurance companies.
- Other bodies of the Public Administration.

10.- International transmissions

This section should reflect the countries and categories of the parties to which the data are assigned and that do not form part of the European Economic Area.

ANNEX VI[6]

Clause relating to the processing of personal data– Party in charge of processing

1. The provider undertakes to keep the information classified as confidential in the maximum confidence and secrecy. Any information to which the provider may have access under the present contract, in particular, information and data of the laboratory which it may have accessed during the its performance. The provider undertakes not to disclose any confidential information or publish it directly through third parties or companies or to make it available to third parties without the prior written consent of the laboratory.

2. Similarly, the provider undertakes, following the termination of the present contract, not to keep any copy whatsoever of the confidential information.

3. The provider will inform its personnel and collaborators of the obligations contained in the present contract on confidentiality. The provider will make whatsoever warnings and enter into whatsoever documents as may be necessary with his personnel and collaborators in order to ensure compliance with such obligations.

4. The provider recognises that personal data protection legislation lays down a series of obligations in the processing of personal data, including the prohibition to assign personal data without the pertinent authorisation of the owner of the personal data. For such purposes, the provider should fulfil the following obligations:

    a) The provider will keep the personal data accessed hereunder in the strictest reserve and confidence.

    b) The provider will only process such data in accordance with the laboratory's instructions.

    c) The provider will not apply or use the data for purposes other than those that figure in the contract and will not report them, not even for storage, to other persons.

    d) The provider will observe the security measures laid down in the laboratory's Security Document when providing its services at the laboratory's facilities.

    e) In no event will the provider store the data on portable devices and not will he process them off the laboratory's premises.

    f) Once the contract services have been completed, the personal data should be destroyed and/or returned by the provider together with any carrier media or documents in which any personal data processed figure.

[6] *The content of this Annex will be fulfilled on a case by case basis.*

5. The laboratory may carry out an audit of the provider's actions in order to verify the fulfilment of the obligations contained in this clause. Such audit may be conducted without prior warning and will be payable by the laboratory.

6. The provider may in no event subcontract the services under the present contract.

7. Nonetheless, the provider is expressly authorised to act on account and behalf of the laboratory and to subcontract the provision of the Clinical research services provided that:

   - The processing of the personal data by the subcontractor conforms to the laboratory's instructions.

   - The provider undertakes to formalise with the subcontractor a contract commissioning the processing of personal data in accordance with Article 12 of Organic Law 15/1999 on personal data protection and transfer the same obligations as those contained in this contract.

   If the subcontractor cannot be identified at the time this contract is entered into, the provider will have to inform the laboratory prior to the subcontracting of the identity of the company which it will subcontract, which will be considered "In charge of Processing" for the purposes provided in the LOPD with respect to the laboratory.

8. Non-compliance by the provider of any of the obligations contained in this clause will make him directly liable for any violations and will obligate him to indemnity the laboratory for the damages caused.

9. The confidentiality obligations contained in this contract will be for an indefinite duration and will remaining effect after the termination, for any cause, of the relationship between the laboratory and provider.

5.2. PHARMACOVIGILANCE ACTION PROTOCOL

I. Introduction and scope of application

II. Pharmacovigilance using dissociated data (DD)

1. Dissociation procedure

1.1. Notification of adverse reactions by healthcare professionals.
1.2. Notification of adverse events by consumers, consumers' legal representatives or other reporters.

2.Exercise of ARCO rights

3.Security measures

4.Third-party access to data

5.International transfers

III. Pharmacovigilance using personal data (PD)

Notification of adverse events by consumers, consumers' legal representatives or other reporters.

1. By telephone
2. By electronic mail, through the company's website applications, by post or by fax
3. Exercise of ARCO rights
4. Security measures
5. Third-party access to data
6. International transfers

Annex I: Clause on personal data processing: party in charge of processing.

Annex II: Pharmacovigilance file (PVF).

Annex III: Confidentiality clause – Personnel with access to personal data.

I. INTRODUCTION AND SCOPE OF APPLICATION.

The purpose of this Action Protocol is to establish the guidelines that must be followed by pharmaceutical laboratories when processing identification data and health information of consumers that have experienced adverse events while being treated with products sold by the laboratories, and the identification data of reporters other than consumers, involving any kind of carrier media and processing method, whether automated or otherwise, in conformity with the following basic regulations:

- Organic Law 15/1999, of 13 December 1999, on Personal Data Protection (LOPD).
- Law 29/2006, of 26 July 2006, on guarantees and the rational use of medicinal products and medical devices.
- Royal Decree 1720/2007, of 21 December 2007, whereby the Enabling Regulations for Organic Law 15/1999, of 13 December 1999, on Personal Data Protection (LOPD) were introduced.
- Royal Decree 1344/2007, of 11 October 2007, regulating pharmacovigilance of medicinal products for human use.
- Volume 9A of The Rules Governing Medicinal Products in the European Union. Guidelines on Pharmacovigilance for Medicinal Products for Human Use.

Pharmacovigilance is the public healthcare activity performed to identify, quantify, evaluate and prevent risks associated with the use of medicinal products available in the market.

One of the pharmacovigilance tools employed to monitor medicinal product safety is spontaneous notification, based on the communication, collection and assessment of notifications of suspected adverse reactions to medicinal products submitted by healthcare professionals. Healthcare professionals report the suspected adverse reactions that they deem most relevant (e.g. reactions that are serious or caused by recently launched medicinal products) to Regional Pharmacovigilance Centres or to the pharmaceutical laboratories.

Article 53.3 of Law 29/2006, of 26 July 2006, on guarantees and the rational use of medicinal products and medical devices requires pharmaceutical laboratories to notify the Regional Health Authorities of suspected adverse reactions of which they are aware and that could have been caused by medicinal products that they manufacture or sell, in accordance with pharmacovigilance good practices. Additionally, laboratories must continuously update product safety information, implement pharmacovigilance plans and risk management programmes, and evaluate the medicinal product's benefit/risk profile, pursuant to national and European guidelines.

Royal Decree 1344/2007, of 11 October 2007, on pharmacovigilance of medicinal products for human use includes, among laboratory obligations, the reporting to the AEMPS of all suspected adverse reactions in a periodic safety Update report.

Expedited reporting

Laboratories have a number of pharmacovigilance obligations under applicable regulations, including the detailed registration of all suspected adverse reactions reported to company personnel, including sale representatives, by healthcare

professionals working in Spain. Reactions that are deemed to be serious must be reported without delay to the Authorities of the region in which the healthcare professional is based.

When the laboratory requires additional information on a specific case, it contacts the healthcare professional directly and does not need the identification details of the subject that experienced the reaction, as these data add no scientific value to the notification.

In order to perform its functions, the laboratory must designate a person in Spain to be permanently responsible for pharmacovigilance, who must form part of the Pharmacovigilance Unit.

This unit is formed by personnel employed by the laboratory and/or by personnel employed by a CRO contracted by the laboratory.

Other notifications

In addition to collecting notifications from healthcare professionals of suspected adverse reactions, there are laboratories that, due to internal company policy or because they follow the pharmacovigilance recommendations provided by Volume 9A of The Rules Governing Medicinal Products in the European Union, register all untoward medical occurrences affecting a subject treated with a product, which do not necessarily have a causal relationship with the product (adverse event). These notifications are not communicated expeditiously to the health authorities but are included in the periodic product safety reports submitted to the health authorities.

Notifications that are reported directly by consumers or other reporters (family members, close friends) may be registered by the laboratory using dissociated data since the subject's identification data are not necessary to evaluate the case. However, there are laboratories that, due to company policy and Volume 9A recommendations, have put a follow-up procedure in place and therefore register the personal data of consumers, legal representatives and other reporters.

Pharmacovigilance data sources may be healthcare professionals or reporters (a person who is not a healthcare professional that reports an adverse event to the Pharmacovigilance Unit):

- **Healthcare professional:** Doctors, pharmacists, dentists, nurses and other healthcare professionals who are required, among other obligations, to report suspected adverse reactions to any product marketed by a pharmaceutical laboratory.
- **Consumer:** Persons other than the healthcare professional who experience an adverse event while using a product marketed by a pharmaceutical laboratory.
- **Consumer's legal representative:** Persons who, on behalf of a disabled person or minor, report the event experienced by the consumer to the Pharmacovigilance Unit.
- **Other reporters:** Persons that are not healthcare professionals and are not included in the previous paragraphs who report to the Pharmacovigilance Unit an adverse event experienced by a consumer, e.g. family members or close friends.

5.2- PHARMACOVIGILANCE ACTION PROTOCOL.

The ordinary means of reporting adverse events and/or reactions are as follows:

1. **Telephone.** Calls may be received directly by the Pharmacovigilance Unit, by a different department, by the switchboard or by the laboratory's call centre service.
2. **Electronic mail.** E-mails may be received by the Pharmacovigilance Unit or by any other laboratory department.
3. **Laboratory website applications.** The information from these applications is generally accessed by several laboratory departments.
4. **Post or fax.** Letters and/or faxes may be received directly by the Pharmacovigilance Unit or by a different laboratory department.

As a general principle, already mentioned above, pharmacovigilance obligations may be fulfilled without any need to obtain the identification data of the consumers or reporters in the terms described above.

Nonetheless, there are laboratories that, in order to comply with the guidelines contained in Volume 9A of The Rules Governing Medicinal Products in the European Union, need to perform a follow-up of notifications and therefore require the personal data of consumers, their legal representatives or other reporters. This Action Protocol therefore addresses separately pharmacovigilance using dissociated data and pharmacovigilance using personal data.

II. PHARMACOVIGILANCE USING DISSOCIATED DATA (DD).

This section comprises the following points:

1. Dissociation procedure:

1.1. Notification of adverse reactions by healthcare professionals (DD)

1.2. Notification of adverse events by consumers, consumers' legal representatives or other reporters (DD)
- By telephone (DD)
- By electronic mail or through laboratory website applications (DD)
- Using a specific notification form, by post or fax (DD)

2. Exercise of the rights of access, rectification, cancellation and opposition.

3. Security measures.

4. Third-party access to data.

5. International transfers.

The procedure to be followed by pharmaceutical laboratories that decide not to access the identification data of the consumers of their products and contact the pharmacovigilance unit directly or through a reporter is described first. The procedure that would be applied to notifications received from healthcare professionals where the identification data of the persons involved in a suspected adverse reaction are not necessary is also described.

Responsibility for the dissociation procedure applied pertains to both the healthcare professional that reports the reaction and to the personnel of the pharmacovigilance unit who receive the notifications.

The persons responsible for ensuring that the data are dissociated are subject to a principle of absolute independence and must undertake to act at all times using their own criteria in the course of their work, without accepting any kind of instruction or suggestion relating to the registration of the consumer's identification data.

In order to guarantee the independence of pharmacovigilance service personnel, pharmaceutical laboratories are required not to dismiss or penalise their personnel if they refuse to register personal data of the consumer and/or reporters.

1. Dissociation procedure

1.1. Notification of adverse reactions by healthcare professionals (DD)

a) The laboratory will not participate directly in the collection of data or access the documents and/or files containing the clinical record that includes the consumers' identification data.

b) The laboratory will inform the healthcare professionals that they must not send the consumers' identification details in their notifications.

c) The laboratory will ask the healthcare professional to check, when preparing the notification, that no information has been included which could allow the consumer to identify the consumer. In this respect, no numerical, alphabetic, graphic, acoustic or other type of information that could allow the consumer to be identified may be included in the notification.

In particular, the healthcare professional must provide the following information in relation to the adverse reaction experienced by the consumer:

- Place of origin of the suspected adverse reaction.
- Patient's date of birth, age, gender, weight and height.
- Description of the reaction, its seriousness and the outcome.
- Treatment suspected to have caused the reaction, concomitant treatment and treatment administered to treat the reaction.
- Personal history, concomitant illnesses and diagnostic tests.
- Information from the healthcare professional to allow case follow-up.

In order to guarantee that the data relating to an adverse reaction included in the laboratory's data collection system do not contain the consumer's personal data, the personnel of the pharmacovigilance unit will follow a different procedure depending on the means used by the healthcare professional to report the suspected adverse reaction:

- By telephone. If the healthcare professional provides any kind of consumer personal data, the pharmacovigilance unit personnel must not register the data in any event in the laboratory's data collection system.

- By e-mail or laboratory website applications. The pharmacovigilance unit personnel will print the e-mail or information reported through the laboratory's website, will cross out the consumer's personal data and will not register the data in any event in the laboratory's data collection system. The e-mail will then be deleted from the computer or the information will then be deleted from the website application.

- Using a specific laboratory notification form, by post or by fax. If the healthcare professional provides any kind of consumer personal data, the pharmacovigilance unit personnel will remove it from the form received by post or fax and will not register the data in any event in the laboratory's data collection system.

Finally, with respect to the healthcare professional's contact data, he or she will be informed as follows:

- Existence of a personal data file or personal data processing; the purpose of the collection of the data (to know who has reported the case and to perform an adequate follow-up) and the recipients of the information (Pharmacovigilance Unit and, *if applicable, the group's international companies or other companies with which it has entered into selling licences or agreements for the preparation of Periodic Safety Update Reports).*

- The optional nature of his or her reply to the questions posed and the consequences of the obtainment of the data or the refusal to supply the data.

- Possibility of exercising the rights of access, rectification, cancellation and opposition.

- Identity and address of the party responsible for data processing or, if applicable, of its representative.

As an example, the healthcare professional may be informed in the following terms:

> *"In accordance with regulations on healthcare and data protection, the personal data that you provide us with will be included in the pharmacovigilance file to be analysed and to send to the health authorities information on the suspected adverse reactions that you have reported, and to follow up on your report. You may exercise your rights of access, rectification, cancellation and opposition with respect to your data at the following address..... (If applicable: Your personal data may also be held or kept by the group's international companies and by companies with which we have entered into selling licences or agreements for the preparation of Periodic Safety Update Reports, for the same purpose, to which you consent. You may consult the group companies to which your data will be assigned and the countries in which those companies are domiciled in the laboratory's website").*

1.2. Notification of adverse events by consumers, consumers' legal representatives or other reporters (DD).

a) The personnel of the pharmacovigilance unit will be informed of the laboratory's decision not to collect identification data of the consumer, consumer's legal representative or other reporter.

b) The personnel of the pharmacovigilance unit will be responsible for ensuring that the following data are registered in the laboratory's data collection system in relation to the adverse event experienced by the consumer:

   - Place of origin of the adverse event.
   - Patient's date of birth, age, gender, weight and height.
   - Description of the event, its seriousness and the outcome.
   - Treatment suspected to have caused the adverse event, concomitant treatment and treatment administered to treat the event.
   - Personal history, concomitant illnesses and diagnostic tests.
   - Information on the healthcare professional to allow follow-up.

In order to guarantee that the data relating to an adverse event included in the laboratory's data collection system do not contain personal data, the personnel of the pharmacovigilance unit will follow a different procedure depending on the means used by the consumer, consumer's representative or other reporter to report the adverse event:

- By telephone (DD). If the consumer, consumer's representative or other reporter provides any kind of personal data, the pharmacovigilance unit personnel must not register the data in any event in the laboratory's data collection system.

The consumer, consumer's representative or other reporter will be informed of the importance of contacting the healthcare professional responsible for the consumer's clinical follow-up and, subsequently, the professional's name and healthcare centre will be requested; the consumer, consumer's representative or other reporter will be asked to contact the laboratory again if any additional information is obtained on the adverse event experienced by the consumer.

- By e-mail or laboratory website applications (DD). The pharmacovigilance unit personnel will print the e-mail or information reported through the laboratory's website, will cross out the personal data contained in the information and will not register the data in any event in the laboratory's data collection system. The e-mail will then be deleted from the computer or the information will then be deleted from the website application.

- Using a specific laboratory notification form, by post or by fax (DD). If the consumer, consumer's representative or other reporters provides any kind of personal data, the pharmacovigilance unit personnel will remove it from the form received by post or fax and will not register the data in any event in the laboratory's data collection system.

c) The laboratory may perform periodic checks to confirm that the pharmacovigilance service has no data that allow the consumers affected by a notification to be identified.

2. Exercise of rights of access, rectification, cancellation and opposition (ARCO).

Through the dissociation procedure described above, the laboratory will not hold the personal data of consumers, consumers' representatives or other reporters.

Nonetheless, the laboratory is required to respond to any request received in any event, irrespective of whether or not the personal data of reporters are included.

The pharmaceutical laboratory must follow the procedure stipulated in the ARCO Rights Action Protocol in relation to the exercise of ARCO rights.

Moreover, with respect to the healthcare professional whose data are registered, pursuant to subsection II.1.1 of this Protocol, the provisions of the ARCO Rights Action Protocol must be observed.

3. Security measures.

Pharmaceutical laboratories that have followed the dissociation procedure described above will not be required to apply security measures to the dissociated data on consumers, consumers' representatives or other reporters.

With respect to the data of the healthcare professional that are registered, pursuant to subsection II.1.1. of this Protocol, the basic level security measures must be applied. In this respect, the pharmaceutical laboratory must have a security document containing the technical and organisational measures that must be fulfilled by all persons that access the personal data in the file containing the data of the healthcare professional,

as stipulated in Article 88 RLOPD. The security document must indicate all the security measures applicable under Title VIII RLOPD.

4. Third-party access to data.

Pharmaceutical laboratories that have followed the dissociation procedure provided in this Action Protocol may freely communicate the dissociated data on consumers, legal representatives and other reporters to any individuals or legal entities.

The following guidelines must be followed in relation to the personal data of healthcare professionals:

4.1. Assignment of processing.

On occasions, third parties may access the personal data of the healthcare professionals in order to provide a service. In the field of pharmacovigilance, such services are usually provided by a CRO.

In the event of a provision of services in the terms referred to in the preceding paragraph, a contract must be concluded between the laboratory and the provider, as the party in charge of processing, stipulating that the provider will only process the data as instructed by the laboratory, that the data will not be applied or used for any purpose other than the one stated in the contract, and that the data must not be communicated to other persons, not even for preservation.

The contract will also stipulate the data security level and the data security measures that the provider is required to implement.

Once the contracted service has been provided, the personal data must be returned to the party responsible for the file and/or eliminated from any system, together with all carrier media or documentary support containing any personal data processed.

In the event that the party in charge of processing uses the data for other purposes, discloses the data or uses the data in breach of the contract, it will also be deemed responsible for processing and will be answerable for the infringements personally committed.

Annex I contains the model clause on personal data processing to be used when contracting a CRO to provide pharmacovigilance services, taking into account the special duty of secrecy to which the personnel contracted through a CRO are subject.

4.2. Disclosure to other group companies or third companies.

The disclosure of personal data to other group companies or to third companies requires the unequivocal and individualised consent of the affected party (healthcare professional). The list of companies must be easily accessible for consultation by the affected party (e.g. website) or consent must be obtained to disclose the personal data to the pharmaceutical companies of the same business group or to third companies, for the same personal data processing purposes.

4.3. Disclosure to the parent company.

The disclosure of personal data to the parent company in order to comply with selling licences or to prepare Periodic Safety Update Reports requires the unequivocal consent of the affected party (healthcare professional). In this regard, the issue of whether the company is located in a country in which personal data protection measures are comparable to those in place in Spain must be considered.

If disclosure to the parent company takes place under a contract for the provision of services, the affected party (healthcare professional)'s consent will not be necessary but the rules applicable to the parties in charge of processing will be applicable (see subsection 4.1 of this Action Protocol).

In the event that the data disclosed to the parent company are not personal data due to being dissociated, aggregated or statistical, or any other information that, in accordance with the Law, is not deemed to include personal data, the provisions of this subsection and of subsections 4.2, 4.4 and 4.5 will not apply.

4.4. Notifications stipulated by law.

The affected party (healthcare professional)'s consent will not be required for data communications to the national or international health authorities under pharmacovigilance regulations.

5.- International transfers.

Cases in which a laboratory, through its pharmacovigilance unit, wishes to make an international data transfer will relate only to the personal data of healthcare professionals that report an adverse reaction to a parent company headquartered outside the European Economic Area. Such international transfers are regulated by the internal policies of the laboratory's business group.

In the event that such transfers are effected, the following considerations must be observed:

A distinction must be made between international transfers to States that provide an adequate level of protection and to States that do not have a level of protection that is comparable with the level in Spain.

a) States that provide an adequate level of protection

States that provide an adequate level of protection are those that have been declared by the European Commission, through its reports, or by the Spanish Data Protection Agency, through rulings published in the Official State Journal, to guarantee an adequate level of protection.

Additionally, the group of States that provide an adequate level of protection must also include US entities adhered to the "Safe Harbour Agreement", which arose from the need to bring EU data protection regulations into line with the procedures of US companies, in which data protection is treated differently to the treatment afforded under the European system.

For this reason, this agreement was approved by the European Commission in 2000, having been prepared by the US Department of Commerce. All companies and entities that adhere to the agreement will be understood to provide protection that is comparable to that required under EU legislation, permitting the flow of data between these companies and other entities from European Union Member States.

If the destination of the international transfer is a country with an adequate level of protection, the only requirement will be the submission of a notification to the General Data Protection Registry.

The updated list of countries providing a comparable level of protection is available in the Spanish Data Protection Agency's website (www.agpd.es).

b) States that do not provide an adequate level of protection

Data transfers to countries without an adequate level of protection require prior authorisation from the Director of the Spanish Data Protection Agency. This authorisation is obtained by means of the procedure stipulated in the RLOPD (Articles 137 to 144).

Laboratories may, however, make transfers to countries that do not provide an adequate level of data protection without any need to request prior authorisation from the Agency Director, provided the international data transfer is effected in any of the following circumstances:

- Transfers resulting from the application of Treaties or Conventions to which Spain is party.
- For reasons of international judicial assistance, health (healthcare and prevention) or the recognition, exercise or defence of a right in a court action.
- At the request of the party having a legitimate interest and of a Public Registry, in accordance with the purpose of that interest.
- The affected party's prior and unequivocal consent to the transfer. In general, prior and unequivocal consent of the healthcare professional must be obtained by means of the clause contained in II.1.1., particularly informing the healthcare professional that:

  "Your personal data may also be held or kept by the group's international companies and by companies with which we have entered into selling licences or agreements for the preparation of Periodic Safety Update Reports, for the same purpose, to which you consent. You may consult the group companies to which your data will be assigned and the countries in which those companies are domiciled in the laboratory's website".

  In the event that the healthcare professional's consent has not been obtained in the manner stated in the above-mentioned clause, authorisation must be obtained from the Director of the Spanish Data Protection Agency for the international transfer of the healthcare professional's data to States that do not provide an adequate level of protection.

In these exceptional cases, the obligation to submit a notification to and register the international transfer with the General Data Protection Registry must also be observed.

c) Corporate Binding Rules

In international transfers of data to States that do not provide an adequate level of protection, there are specific provisions for transfers of data between companies located in different States that form part of the same multinational group.

In such cases, the Agency Director may authorise international transfers within a multinational group of companies provided that group has adopted a number of internal corporate binding rules, for all the group companies, that guarantee the fulfilment of the principles and exercise of the rights recognised by the LOPD.

III. PHARMACOVIGILANCE USING PERSONAL DATA (PD).

This section is divided into the following points:

Notification of adverse events by consumers, consumers' legal representatives or other reporters.

1. By telephone (PD)

1.1. Call answering procedure

1.2. Filing and preservation

2. By electronic mail, through the company's website applications, by post or fax (DP).

2.1. Procedure for the receipt of information supplied by e-mail, through website applications, by post or by fax sent by reporters who are not healthcare professionals

2.1.1. The reporter is the legal representative of the consumer who has experienced the adverse event

2.1.2. The reporter is not the legal representative of the consumer who has experienced the adverse event

2.2. Filing and preservation

3. Exercise of rights of access, rectification, cancellation and opposition (ARCO)

4. Security measures

5. Third-party access to data

6. International transfers

There follows a description of the procedure that must be followed by the laboratory when processing the personal data of consumers, consumers' legal representatives or other reporters of adverse events, without prejudice to the exceptions envisaged by the Law.

As explained at the start of this Protocol, pharmacovigilance obligations may be fulfilled without obtaining the identification data of consumers, consumers' legal representatives or other reporters. However, as stipulated in Royal Decree 1344/2007 on pharmacovigilance of medicinal products for human use, the European Commission has prepared and published the guidelines contained in Volume 9A of The Rules Governing Medicinal Products in the European Union, which will be applicable together with successive updates of the guidelines. The guidelines indicate how cases received from consumers and other non-Clinical sources must be handled, including the follow-up of the case with a healthcare professional and the receipt of medical documentation supporting the suspected adverse reaction. For this reason, there are laboratories that, in order to follow these guidelines, consider it necessary to register data on consumers, consumers' legal representatives or other reporters.

Moreover, there are other uncommon and exceptional cases in which laboratories engaged in pharmacovigilance activities using dissociated data access consumer identification data.

Although the probability of the occurrence of such cases is minimal, a theoretical analysis may identify the following exceptions:

- Extraordinary event beyond the control of laboratory management that generates the need to identify the consumer.
- Harm to the consumer giving rise to the obligation to pay damages.
- Human error.

In such cases, laboratories will apply the appropriate measures to avoid the identification of the consumer, including:

- Management of notifications only through the Pharmacovigilance Unit.
- Processing of the consumer's compensation through the insurance company.
- Standard operating procedure designed to prevent human error.
- Personal data filtering system.

If, despite the application of these preventive measures, the laboratory becomes aware of the consumer's identity, the laboratory may choose between the following options:

- Apply high-level security measures to the file and fulfil the requirements of the Law on Personal Data Protection (LOPD).
- Create a specific high-level file in a computer not connected to the system that contains the data of the persons whose identification data are known by the laboratory. If the laboratory opts to create a specific file, it will be governed by the provisions of this Protocol in relation to pharmacovigilance using personal data.
- Delete the identification data of the affected person.

To conclude, the provisions of this section in relation to pharmacovigilance using personal data are applicable to the following cases:

- Laboratories that have decided to obtain the personal data of consumers and/or other reporters.
- Laboratories with a pharmacovigilance unit engaged in processing dissociated data that have obtained the identification data of consumers in any of the exceptional cases referred to above.

Finally, if the adverse reaction is reported by a healthcare professional, the provisions of section II (Pharmacovigilance using dissociated data) will be applicable.

Notification of adverse events by consumers, consumers' legal representatives or other reporters (PD).

Pharmacovigilance file

Given that laboratories, in the "pharmacovigilance using personal data" scenario, process personal data as a result of the notification and follow-up of adverse events, it should be noted that the party responsible for the pharmacovigilance file is the laboratory that has the pharmacovigilance unit and, as such, the laboratory must

declare the relevant file (Pharmacovigilance file: PVF) to the Spanish Data Protection Agency before the file is created.

The typical structure of a PVF, the purpose of which is to receive and follow up on adverse events experienced by consumers of the laboratory's products, is described in **Annex II**. It should be noted that the structure reflected in that Annex is illustrative and must be adapted based on the information obtained by each laboratory in relation to an adverse event.

Additionally, the general structure of laboratory personal data files relates to the purpose of the data processing and therefore a single pharmacovigilance file will be declared that, in conceptual terms, will contain the data of the persons that have reported an adverse event.

Pharmacovigilance personnel must only collect data that are strictly necessary to document the adverse event that has occurred and to obtain the best possible information on the safety of the product in question in order to allow the appropriate measures to be adopted.

It should be noted that the personal data are collected to comply with laws or regulations and/or to receive or follow up on what could be a medical emergency, by personnel subject to a duty of secrecy inherent in their professional, which is backed up in this case by confidentiality clauses signed by that professional. Consequently, pursuant to Articles 6.1. and 7.6. LOPD, the consumer's prior and unequivocal consent will not be necessary.

This does not exonerate the personnel in pharmacovigilance units who collect the personal data from applying particular diligence in the fulfilment of the information obligations relating to personal data treatment, with respect to consumers, consumers' legal representatives and other reporters.

Beyond the confidentiality obligations applicable to pharmacovigilance unit personnel contained in the relevant employment contracts with laboratories or, if applicable, with CROs, all the personnel of a pharmacovigilance unit must sign a clause that is similar to the one attached as **Annex III** to this Action Protocol.

The data collection procedures to be applied, depending on the type of notification method used by consumers and/or reporters to report adverse events, are as follows:

1.- By telephone (PD)

The following must be considered:

1.1. Call answering procedure (by personnel outside or inside the Pharmacovigilance Unit).

1.2. Filing and preservation.

1.1. Procedure for answering calls from consumers, consumers' legal representatives or other reporters.

Bearing in mind that the call to the laboratory may be answered using a telephone that is not in the pharmacovigilance unit, set out below is a description of the data collection procedure to be followed by laboratories adhered to the Standard Code:

A. Calls answered by personnel outside the Pharmacovigilance Unit:

Procedure

A.1. Transfer the call to the pharmacovigilance unit.

A.2. Where the call cannot be transferred, the person that answers will request the reporter's name, telephone number and the reason for the call. The reporter will also be informed that the pharmacovigilance unit will contact him or her to obtain additional information. The pharmacovigilance unit will be informed of the call.

B. Calls answered by Pharmacovigilance Unit personnel:

Procedure

B.1. Answer the reporter's call, the person that answers identifying himself or herself (full name, post and department), or contact the reporter if the transfer of the call was not previously possible.

B.2. Depending on the type of reporter, the following procedure will be followed:

B.2.1. The reporter is the legal representative of the consumer who has experienced the adverse event:

- Collect the consumer's personal health information, as necessary to describe the adverse event and register the data.
- Inform the reporter of the importance of contacting the healthcare professional responsible for clinical follow-up and then request the professional's name and healthcare centre. If it is possible to contact the healthcare professional, the personal data protection recommendations contained in subsection II-1.1 must be applied.
- Inform the reporter as follows:
  - Existence of a personal data file or processing, purpose of the collection of the data (analyse safety information and follow up on the case) and recipients of the information (pharmacovigilance unit).
  - Optional nature of his or her reply to the questions posed and consequences of the obtainment of the data or of the refusal to provide the data.
  - Possibility of exercising the rights of access, rectification, cancellation and opposition.

- Identity and address of the party responsible for data processing or, if applicable, its representative.

As an example, the consumer or consumer's legal representative may be informed in the following terms:

> *"In accordance with regulations on healthcare and data protection, the personal health information that you provide us with will be included in the company's pharmacovigilance file to be analysed and to send to the health authorities information on the adverse events that you have reported, and to follow up on the case. You may exercise your legal rights of access, rectification, cancellation and opposition with respect to your data at the following address..... and in accordance with healthcare regulations (If applicable: Your personal data may also be held or kept by the group's international companies and by companies with which we have entered into selling licences or agreements for the preparation of Periodic Safety Update Reports, for the same purpose, to which you consent. You may consult the group companies to which your data will be assigned and the countries in which those companies are domiciled in the laboratory's website").*

B.2.2. The selling *licences* reporter is the legal representative of the consumer who has experienced the adverse event:

Option one:

- Inform the reporter that Law 29/2006, of 26 July, on guarantees and the rational use of medicinal products and medical devices permits the processing of consumers' personal health data without any need to obtain consent.

- If the consumer can finally be persuaded to speak over the telephone to continue the conversation, the procedure provided in subsection B.2.1. will be followed.

- If the consumer cannot be persuaded to participate in the telephone conversation, the procedure described in option two will be followed.

Option two:

- Take note of the reporter's data and of the adverse event experienced by the consumer, without registering in any event the consumer's personal data.

- Inform the reporter of the importance of contacting the healthcare professional responsible for the consumer's clinical follow-up and request the professional's name and healthcare centre to follow up on the case. If it is possible to contact the healthcare professional, the personal data protection recommendations contained in subsection II-1.1 must be applied.

- Inform the reporter of the inclusion of his or her data in a file and of his or her rights under the LOPD:

- Existence of a personal data file or processing, the purpose of data collection (case follow-up) and the recipients of the information (pharmacovigilance unit).
- Optional nature of his or her reply to the questions posed and consequences of the obtainment of the data or of the refusal to provide the data.
- Possibility of exercising the rights of access, rectification, cancellation and opposition.
- Identity and address of the party responsible for data processing or, if applicable, its representative.

As an example, the reporter may be informed as follows:

"In accordance with data protection regulations, the personal data that that you provide us with will be included in the company's pharmacovigilance file to follow up on the information you have reported. You may exercise your legal rights of access, rectification, cancellation and opposition with respect to your data at the following address..... and in accordance with healthcare regulations (If applicable: Your personal data may also be held or kept by the group's international companies and by companies with which we have entered into selling licences or agreements for the preparation of Periodic Safety Update Reports, for the same purpose, to which you consent. You may consult the group companies to which your data will be assigned and the countries in which those companies are domiciled in the laboratory's website").

1.2. Filing and preservation.

The form used to collect the data of the consumer, consumer's legal representative or other reporter will form part of the notification file and the preservation rules stipulated in the Standard Code of which this Action Protocol forms part will be observed.

In particular, and in line with sector practices and customs, this documentation will be kept for at least five years after the end of the period during which the product referred to in the notification is in the market.

2. By electronic mail, through the company's website applications, by post or by fax (DP).

The following will apply:

2.1. Procedure for receiving information supplied by e-mail, website applications, post or fax

2.1.1. The reporter is the legal representative of the consumer who has experienced the adverse event.

2.1.2. The reporter is not the legal representative of the consumer who has experienced the adverse event.

2.2. Filing and preservation

2.1. Procedure for receiving information by e-mail, website applications, post or fax from reporter who are not healthcare professionals.

As stated at the start of the Protocol, letters, faxes, company website information and e-mails may be received by the pharmacovigilance unit or by any other laboratory department.

In the event that they are received by a different department, the information must be forwarded to the pharmacovigilance unit.

The department that first receives the information must check that it has been correctly received by the pharmacovigilance unit.

In the case of an e-mail, once correct receipt has been acknowledged by the pharmacovigilance unit, the department that initially received the information will delete the e-mail.

Once the pharmacovigilance unit has the information, either because it was received directly by the unit or forwarded by a different department, the following procedure will be followed, depending on the type of reporter:

2.1.1. The reporter *is the legal representative of the consumer who has experienced the adverse event:*

- Register the reporter's personal health data.
- Reply to the reporter by e-mail, letter, fax or the laboratory's website application, providing the following information:
  - Importance of contacting the healthcare professional responsible for clinical follow-up (and then request the professional's name and healthcare centre). If it is possible to contact the healthcare professional, the personal data protection recommendations contained in subsection II-1.1 must be applied.
  - Existence of a personal data file or processing, purpose of the collection of the data (case follow-up) and recipients of the information (pharmacovigilance unit).
  - Optional nature of his or her reply to the questions posed and consequences of the obtainment of the data or of the refusal to provide the data.
  - Possibility of exercising the rights of access, rectification, cancellation and opposition.
  - Identity and address of the party responsible for data processing or, if applicable, its representative.

As an example, the consumer or consumer's legal representative may be informed in the following terms:

"In accordance with regulations on healthcare and data protection, the personal health information that you provide us with will be included in the company's pharmacovigilance file to be analysed and to send to the health authorities information on the adverse events that you have reported, and to follow up on the case. You may exercise your legal rights of access, rectification, cancellation and opposition with respect to your data at the following address..... and in accordance with healthcare regulations (If applicable: Your personal data may also be held or kept by the group's international companies and by companies with which we have entered into selling licences or agreements for the preparation of Periodic Safety Update Reports, for the same purpose, to which you consent. You may consult the group companies to which your data will be assigned and the countries in which those companies are domiciled in the laboratory's website").

2.1.2. The reporter *is not the legal representative of the consumer who has experienced the adverse event.*

Reply to the reporter by e-mail, letter, fax or the laboratory's website application, providing the following information:

- The laboratory will only register the consumer's health data and the reporter's personal data.
- Importance of contacting the consumer directly and of knowing the name and healthcare centre of the healthcare professional responsible for the consumer's clinical follow-up, requesting the name and centre for follow-up purposes. If it is possible to contact the healthcare professional, the personal data protection recommendations contained in subsection II-1.1 must be applied.
- Existence of a personal data file or processing of the reporter's=personal data, purpose of the collection of the data (case follow-up) and recipients of the information (pharmacovigilance unit).
- Optional nature of his or her reply to the questions posed and consequences of the obtainment of the data or of the refusal to provide the data.
    - Possibility of exercising the rights of access, rectification, cancellation and opposition.
    - Identity and address of the party responsible for data processing or, if applicable, its representative.

As an example, the reporter may be informed in the following terms:

"In accordance with data protection regulations, the personal data that that you provide us with will be included in the company's pharmacovigilance file to follow up on the information you have reported. You may exercise your legal rights of access, rectification, cancellation and opposition with respect to your data at the following address..... and in accordance with healthcare regulations (If applicable: Your personal data may also be held or kept by the group's international companies and by companies with which we have entered into selling licences or agreements for the preparation of Periodic Safety Update Reports, for the same purpose, to which you consent. You may consult the group companies to which your data will be assigned and the countries in which those companies are domiciled in the laboratory's website").

2.2. Filing and preservation.

The e-mails, website application information, letters and faxes and, therefore, the data provided by the consumer, consumer's legal representative or other reporter will form part of the notification file.

In line with sector practices and customs, this documentation will be kept for at least five years after the end of the period during which the product referred to in the notification is in the market.

3. Exercise of ARCO rights.

Consumers, legal representatives and other reporters may exercise the rights of access, rectification, cancellation and opposition. Such requests will be resolved as stipulated in the Action Protocol on ARCO rights, which includes illustrative models for the affected or interested party wishing to exercise any of the above-mentioned rights, and the guidelines to be followed by the parties responsible for the files.

4. Security measures.

Pharmacovigilance units must apply high-level security measures to the data files in which adverse events containing personal data are registered, taking into account the particularly protected nature of the health data reported. The pharmaceutical laboratory will have a security document stating the technical and organisational measures that must be fulfilled by all the persons that access the personal data in the pharmacovigilance file, pursuant to Article 88 RLOPD. This document will indicate all the security measures that are applicable under Title VIII RLOPD.

5. Third-party access to data.

5.1. Party in charge of processing.

On occasions, third parties may access the personal data of the consumers/ reporter in order to provide a service. In the field of pharmacovigilance, such services are usually provided by a CRO.

In the event of a provision of services in the terms referred to in the preceding paragraph, a contract must be concluded between the laboratory and the provider, as the party in charge of processing, stipulating that the provider will only process the data as instructed by the laboratory, that the data will not be applied or used for any purpose other than the one stated in the contract, and that the data must not be communicated to other persons, not even for preservation.

The contract will also stipulate the data security level and the data security measures that the provider is required to implement.

Once the contracted service has been provided, the personal data must be returned to the party responsible for the file and/or eliminated from all systems, together with all carrier media or documentary support containing any personal data processed.

In the event that the party in charge of processing uses the data for other purposes, discloses the data or employs the data in breach of the contract, it will also be deemed responsible for processing and will be answerable for the infringements personally committed.

Annex I contains the model clause on personal data processing to be used when contracting a CRO to provide pharmacovigilance services, taking into account the special duty of secrecy to which the personnel contracted through a CRO are subject.

5.2. Disclosure to other group companies or third companies.

The disclosure of personal data to other group companies or to third companies requires the unequivocal and individualised consent of the affected party (healthcare professional, consumer, legal representative or other reporter). The list of companies must be easily accessible for consultation by the affected party (e.g. website) or consent must be obtained to disclose the personal data to the pharmaceutical companies of the same business group or to third companies, for the same personal data processing purposes.

5.3. Disclosure to the parent company.

The disclosure of personal data to the parent company in order to comply with selling licences, to assess product safety or to prepare Periodic Safety Update Reports requires the unequivocal consent of the affected party (healthcare professional). This consent must consider whether the company is located in a country in which personal data protection measures are comparable to those in place in Spain.

If disclosure to the parent company takes place under a contract for the provision of services, the affected party's consent will not be necessary but the rules applicable to the parties in charge of processing will be applicable (see subsection 4.1 of this Action Protocol).

In the event that the data disclosed to the parent company are not personal due to being dissociated, aggregated or statistical, or any other information that, in accordance with the LOPD, is not deemed to include personal data, the provisions of this subsection and of subsections 5.2, 5.4 and 5.5 will not apply.

5.4. Notifications stipulated by law.

The affected party's consent will not be required for data communications to the national or international health authorities under pharmacovigilance regulations.

Consent will not be necessary when personal health data are assigned to resolve an emergency requiring access to a file or to perform epidemiological studies in the terms stipulated in State or regional healthcare legislation.

6.- International transfers

An international data transfer is any transfer of data from inside the European Economic Area, whether it is a data assignment or a data communication, or where the data are transferred for the account of the party responsible for the file established in Spain.

Cases in which a laboratory could make an international data transfer, through its pharmacovigilance unit, relate to the communication of personal data of healthcare professionals, consumers, legal representatives or other reporters that report an adverse reaction to a parent company headquartered outside the European Economic Area, or to other pharmaceutical companies under selling licences, or for the preparation of Periodic Safety Update Reports. Such international transfers are regulated by the internal policies of the laboratory's business group.

In the event that such transfers are completed, the following considerations and rules must be observed:

A distinction must be made between international transfers to States that provide an adequate level of protection and those that do not have a level of protection that is comparable with the level in Spain.

a) States that provide an adequate level of protection

States that provide an adequate level of protection are those that have been declared by the European Commission, through its reports, or by the Spanish Data Protection Agency, through rulings published in the Official State Journal, to guarantee an adequate level of protection.

Additionally, the group of States that provide an adequate level of protection must also include US entities adhered to the "Safe Harbour Agreement", which arose from the need to bring EU data protection regulations into line with the procedures of US companies, in which data protection is treated differently to the treatment afforded under the European system.

For this reason, this agreement was approved by the European Commission in 2000, having been prepared by the US Department of Commerce. All companies and entities that adhere to the agreement will be understood to provide protection that is comparable to that required under EU legislation, permitting the flow of data between these companies and other entities from European Union Member States.

If the destination of the international transfer is a country with an adequate level of protection, the only requirement will be the submission of notification to the General Data Protection Registry.

The updated list of countries that provide a comparable level of protection is available in the Spanish Data Protection Agency's website (www.agpd.es).

b) States that do not provide an adequate level of protection

Data transfers to countries without an adequate level of protection require prior authorisation from the Director of the Spanish Data Protection Agency. This authorisation is obtained by means of the procedure stipulated in the RLOPD (Articles 137 to 144).

Laboratories may, however, make transfers to countries that do not provide an adequate level of data protection without any need to request prior authorisation from the Agency Director, provided the international data transfer is effected in any of the following circumstances:

- Transfers resulting from the application of Treaties or Conventions to which Spain is party.
- For reasons of international judicial assistance, health (healthcare and prevention) or the recognition, exercise or defence of a right in a court action.
- At the request of the party having a legitimate interest and of a Public Registry, in accordance with the purpose of that interest.
- The affected party's prior and unequivocal consent to the transfer. In general, prior and unequivocal consent of the healthcare professional must be obtained by means of the clause contained in previous sections, particularly informing the healthcare professional, consumer, legal representative or other reporter as follows:

  "Your personal data may also be held or kept by the group's international companies and by companies with which we have entered into selling licences or agreements for the preparation of Periodic Safety Update Reports, for the same purpose, to which you consent. You may consult the group companies to which your data will be assigned and the countries in which those companies are domiciled in the laboratory's website".

  In the event that the healthcare professional, consumer, legal representative or other reporter's consent has not been obtained, authorisation must be obtained from the Director of the Spanish Data Protection Agency for the international transfer of the healthcare professional's data to States that do not provide an adequate level of protection.

In these exceptional cases, the obligation to submit a notification to and register the international transfer with the General Data Protection Registry must also be observed.

c) Corporate Binding Rules

In international transfers of data to States that do not provide an adequate level of protection, there are specific provisions for transfers of data between companies located in different States that form part of the same multinational group.

In such cases, the Agency Director may authorise international transfers within a multinational group of companies provided that group has adopted a number of internal corporate binding rules for all the group companies that guarantee the fulfilment of the principles and exercise of the rights recognised by the LOPD.

ANNEX I

Clause on personal data processing Party in charge of processing[1]

1. The service provider undertakes to treat all the information classified as confidential with the utmost reserve and secrecy. Confidential Information shall be any piece of data that is accessed by the provider under this agreement, particularly information and data owned by the laboratory that are accessed during the performance of this agreement. The provider undertakes not to disclose or publish that confidential information, either directly or through third persons or companies, or to make it available to third parties, without the laboratory's prior written consent.

2. The provider likewise undertakes, following the extinction of this agreement, not to keep any copy of the confidential information.

3. The provider shall inform its personnel and collaborators of the confidentiality obligations stipulated in this agreement. The provider shall issue all notices and sign all documents necessary with its personnel and collaborators to ensure compliance with these obligations.

4. The provider recognises that personal data protection legislation provides a number of personal data processing obligations that include the prohibition on the assignment of personal data without authorisation from the personal data owner. To this end, the provider shall fulfil the following obligations:

   a) The provider shall treat the personal data accessed by virtue of this agreement with the strictest reserve and confidentiality.

   b) The provider shall process the data as instructed by the laboratory.

   c) The provider shall not apply or use the data for any purpose other than the one stated in the agreement and shall not disclose the data to other persons, not even for preservation purposes.

   d) The provider shall implement the security measures stated in the laboratory's Security Document during the provision of its services at the laboratory's facilities.

   e) The provider shall not in any event store the data in handheld devices or process the data outside the laboratory's facilities.

   f) Once the contracted service has been completed, the personal data shall be destroyed and/or returned by the provider, together with any carrier media and documents containing any personal data processed, or returned to the laboratory, in its capacity as the party responsible for the file.

5. The laboratory may audit the provider's activities to verify compliance with the obligations stipulated in this clause. The audit may be performed without prior notice and the audit costs shall be borne by the laboratory.

[1] *The content of this Annex must be adapted to each specific case.*

6. The provider may not in any circumstances subcontract the services that are the object of this agreement.

7. The above notwithstanding, the provider is specifically authorised to act for and on behalf of the laboratory and to subcontract the provision of the pharmacovigilance services, provided that:

   - Personal data processing is performed by the subcontractor in accordance with the laboratory's instructions.

   - The provider undertakes to enter into a personal data processing assignment agreement with the subcontractor pursuant to Article 12 of Organic Law 15/1999 on Personal Data Protection, containing the same obligations stipulated in this agreement.

     If the subcontracted company cannot be identified when this agreement is concluded, the provider shall notify the laboratory, before subcontracting the services, of the identity of the company to be subcontracted, which shall be deemed a "Party in charge of processing" for the purposes of the Data Protection Law (LOPD), vis-à-vis the laboratory.

8. Should the provider fail to fulfil any of the obligations contained in this clause, it shall be directly liable for any infringements committed and shall be required to pay damages to the laboratory.

9. The confidentiality obligations stipulated in this agreement shall have an indefinite duration and shall remain in force following the end of the relationship between the laboratory and the provider, whatever the cause.

ANNEX II

PHARMACOVIGILANCE FILE [2]

1. Information on the party responsible for the PVF

- Company name
- Tax code
- Registered office
- City
- Postcode
- Province
- Country
- Telephone number
- Fax
- E-mail

2. ARCO rights

In the event that the address stated so that the affected parties may exercise their ARCO rights is different from the address of the party responsible for the PVF, this must be indicated.

3. Party in charge of processing

In the event that the Party responsible for the file receives services from a third party which, in order to provide the services, accesses data in the PVF, the PVF registration details must include the following information on the party in charge of processing:

- Company name
- Tax code
- Registered office
- City
- Postcode
- Province
- Country
- Telephone number
- Fax
- E-mail

If there is more than one party in charge of processing and they cannot all be reflected in the relevant register entry, the party whose services will be provided for a longer period or the party that generates the highest risk in terms of the type and volume of data processed should be included.

The content of this section will not affect the obligation whereby a data protection agreement must be concluded between the party responsible for the file and the party in charge of processing, in the terms of Article 12 LOPD and Articles 20 et seq RLOPD.

[2] *The content of this Annex must be adapted to each specific case.*

4. Identity and purpose of the PVF

- File name. The file name could be "Pharmacovigilance File".
- Detailed description of the purpose and intended uses of the "Pharmacovigilance File". The detailed description of the purpose of the file will contain the "Evaluation and follow-up of the adverse events experienced by the consumers of the laboratory's products".

5. Origin of the data

- Interested party. Interested parties are the persons that consume products sold by the laboratory.
- Consumer's legal representative, in the case of consumers who are minors or disabled.
- Other individuals. These persons are the "other reporter", pursuant to the definition contained in this Protocol.
- Other groups. Healthcare professionals, where suspected adverse reactions are reported by these professionals.

6. Type of data, structure and organisation of the PVF

The data that will be obtained from the participating subjects will include the following:

- Health
- Full name
- Address (e-mail)
- Telephone
- Personal characteristics
- Social circumstances (e.g. hobbies and lifestyle)
- Academic and professional
- Other (fax, etc.)

7. Processing system

In general, the documentation generated in connection with the pharmacovigilance activity is processed in both paper format and electronic format and therefore, barring exceptional cases, a **mixed** processing system will be used.

8. Level of security measures

For the processing of health data on product consumers, the level of security measures is **high**.

9. Data assignment or communication

Consumers' data will or may be assigned, at minimum, to the entities and bodies of the public administration.

10. International transfers

This section must include the countries and categories of the recipients to which the data are assigned, outside the countries of the European Economic Area. In particular, international transfers to parent companies located outside the European Economic Area must be included.

ANNEX III

Confidentiality clause – Personnel with access to personal data.[3]

1. The worker undertakes to treat the personal data of the consumers and/or reporters that report adverse events to the pharmacovigilance units, which the worker may access in the course of his or her duties, with the utmost reserve and secrecy, particularly health data. The worker undertakes not to disclose or publish the data, or make it available to third parties, either directly or through third persons or companies.

2. The worker likewise undertakes, following the extinction of this agreement, not to keep any copy of documentation that may contain the personal data of consumers and/or reporters that report adverse events.

3. The worker recognises that personal data protection legislation provides a number of obligations relating to access to personal data. To this end, the worker undertakes to access the personal data of the consumers and/or reporters that report adverse events in accordance with the laboratory's instructions.

4. The confidentiality obligations stipulated in this agreement shall have an indefinite duration and shall remain in force following the end of the employment relationship between the laboratory and the worker.

[3] *The content of this Annex must be adapted to each specific case.*

5.3. DATA PROTECTION PRINCIPLES AND ACTION PROTOCOL FOR THE EXERCISE OF RIGHTS OF ACCESS, RECTIFICATION, CANCELLATION AND OPPOSITION IN PHARMACOVIGILANCE AND CLINICAL RESEARCH USING PERSONAL DATA AND DISSOCIATED DATA

I. Introduction

II. Personal data protection principles

III. Action protocol for the exercise of ARCO rights

1. Introduction and scope of application
2. General considerations
3. Pharmacovigilance using personal data
4. Pharmacovigilance using dissociated data
5. Clinical Research using personal data
6. Clinical Research using dissociated data

Annex I: Exercise of the affected party's rights

Annex II: Model letter informing of the absence of personal data

Annex III: Model reply to a request to exercise the right of access

Annex IV: Model reply to a request to exercise the rights of access, rectification, cancellation and opposition, and revocation of consent (party in charge of processing)

Annex V: Model reply to a request to exercise the right of rectification

Annex VI: Model reply to a request to exercise the right of cancellation

Annex VII: Model confirmation of the end of personal data processing (rights of opposition and revocation)

I. INTRODUCTION.

The purpose of this Protocol is, firstly, to provide the essential principles that must govern the treatment of personal data by laboratories and CROs during clinical research and pharmacovigilance activities.

It also mentions the basic guidelines that must be followed by the parties involved in a clinical research or by pharmacovigilance units in response to requests to exercise the rights of access, rectification, cancellation and opposition by the affected parties (ARCO rights).

Previously, set out below are summary tables clarifying the position of each agent in connection with the files in respect of which, if applicable, the ARCO rights will be exercised:

1. Clinical Investigational File (clinical researches using dissociated data)

LOPD concept	Centre	Sponsor	Monitor	Auditor	Investigator's assistant
Party responsible for file	X				
Party responsible for processing		X			
Party in charge of processing			X	X	X

2. Clinical Investigational File (clinical researches using personal data)

LOPD concept	Centre	Sponsor	Monitor	Auditor	Investigator's assistant
Party responsible for file	X				
Party responsible for processing		X			
Party in charge of processing			X	X	X

3. Case Report Form File (clinical researches using personal data)

LOPD concept	Sponsor	CRO (tasks other than monitoring)
Party responsible for the file	X	
Party responsible for processing	X	
Party in charge of processing		X

4. Pharmacovigilance file (pharmacovigilance using personal data)

The party responsible for the pharmacovigilance file is the laboratory that has the pharmacovigilance unit. The service providers that, during the provision of the service, access personal data in the pharmacovigilance file, will be deemed parties in charge of processing with respect to that file.

LOPD concept	Laboratory	CRO
Party responsible for the file	X	
Party responsible for processing	X	
Party in charge of processing		X

II. PERSONAL DATA PROTECTION PRINCIPLES.

1. Suitability and relevance.

General principle.- The personal data collected from subjects and consumers by laboratories or pharmaceutical companies and CROs that adhere to this Standard Code must be adequate, relevant and not excessive in relation to the scope and the specific, explicit and legitimate purposes for which they are obtained. The personal data will be cancelled when they are no longer necessary or relevant to the purpose for which they were collected or registered.

Clinical research.- The case report form will contain the fields that are strictly necessary to fulfil the objectives of the relevant investigation project. Sponsors that do not need the subject's identification data may opt to apply the dissociation procedure provided in the Action Protocol on Clinical Trials and other Clinical Researches. Once dissociated, the data collected may be processed together with evaluations, comments, reports, statistics, conclusions and any other information that the sponsor considers should be added.

Pharmacovigilance.- The necessary data will be collected to obtain, on a continuous basis, the best possible information on the safety of medicines, thereby allowing the appropriate measures to be taken and, in this way, ensuring that the medicines available in the market show a risk benefit/risk profile that is favourable for the population under the authorised conditions of use[1]. Laboratories that decide to do without the subject's identification data will apply the dissociation procedure provided by the Pharmacovigilance Action Protocol. Once dissociated, the data collected may be processed together with evaluations, comments, reports, statistics, conclusions and any other information that the laboratory considers should be added.

2. Purpose of data collection.

General principle.- The personal data processed may not be used for purposes that are incompatible with the purposes for which the data were collected. The subsequent processing of the data for historical, statistical or scientific purposes will not be deemed incompatible.

Clinical research.- Sponsors that do not require the subject's identification data may apply the dissociation procedure provided in the Action Protocol on Clinical Trials and other Clinical Researches. Once dissociated, the data may be used as the laboratory deems fit.

Pharmacovigilance.- The purpose of data collection will be to identify, quantify, evaluate and prevent risks associated with the use of the products sold by the laboratories that adhere to this Standard Code.

Laboratories that do not require the subject's identification data may apply the dissociation procedure provided in the Pharmacovigilance Action Protocol. Once dissociated, the data may be used as the laboratory deems fit.

[1] Preamble to Royal Decree 1344/2007.

3. Accuracy of data.

General principle.- The personal data will be accurate when obtained, such that they reflect the actual situation. If the personal data registered prove to be inaccurate in whole or in part, or incomplete, steps must be taken to complete them; if this is not possible they will remain unchanged, if necessary for analysis purposes, or they will be cancelled and replaced *ex officio* by the corrected or completed data, without affecting the powers of the data subjects recognised in Article 16 of Organic Law 15/1999, of 13 December 1999, on Personal Data Protection (LOPD).

Clinical research.- The case report form will have a user-friendly format to minimise the risk of error. It will contain the explanations necessary with respect to fields that could generate doubts. Where possible, the options and numerical ranges for the data to be collected will be defined. Electronic case report forms will be equipped with systems to prevent errors, discrepancies and inconsistencies in the data input. Professionals responsible for completing the case report forms will receive the information necessary to complete them as accurately as possible.
Pharmacovigilance.- Data will be collected observing the rules or recommendations designed to guarantee the authenticity and quality of the pharmacovigilance data collected, so as to allow the evaluation at any given time of the risks attributable to the product and the use of consistent criteria when assessing notifications and generating alerts.

4.- Right to Information during data collection.

General principle.- Interested parties who are asked to provide personal data must previously receive the following specific, precise and unequivocal information:

a) Existence of a personal data file or personal data processing, the purpose of the collection of the data and the recipients of the information.

b) Mandatory or optional nature of his or her reply to the questions posed.

c) Consequences of the obtainment of the data or of the refusal to provide the data.

d) Possibility of exercising the ARCO rights.

e) Identity and address of the party responsible for the file or, if applicable, of its representative.

Clinical Research.- The information supplied to the subject participating in a clinical research project will be supplemented by the information stipulated in regulations governing clinical research. The subject will be informed of the assignment of the data to the research sponsor, indicating whether or not the data are assigned in a dissociated form, unless the data have been provided by the subject. The subject may also be informed of the research sponsor's adherence to this Standard Code.

Pharmacovigilance.- Where personal data are obtained from the reporter and/or healthcare professional, they will be informed of the assignment of their data to the laboratory. This information may be supplemented by informing them of the laboratory's adherence to this Standard Code.

5. Affected party's consent.

General principle.- Personal data processing requires the affected party's free, unequivocal, specific and informed consent, unless otherwise stipulated by law.

Clinical research.- The consent of the subject participating in a clinical research project will extend to the provisions applicable to informed consent contained in regulations governing clinical research, which are explained in the Action Protocol on Clinical Trials and other Clinical Researches.

Pharmacovigilance.- The consent of product consumers who report an adverse event will be obtained by the Pharmacovigilance Unit personnel as stipulated in the Pharmacovigilance Action Protocol, barring cases in which the law stipulates that such consent is not required.

6. Specially protected data.

General principle.- Personal data revealing the subject's ideology, union membership, religion and beliefs may only be processed once specific, written consent has been obtained. Personal data referring to the subject's race, health and sex life may only be collected, processed and assigned where this is permitted by law, for general interest reasons, or where specific consent is obtained.

Clinical research.- In addition to the health data, in certain studies it will be necessary to ascertain whether the subject practices any religion that affects his or her eating habits or causes him or her to reject certain medical practices such as blood transfusions. It will also be necessary to know the subject's race and sex life details where required by the clinical research. These data will be collected and processed pursuant to regulations on data protection and clinical research.

Pharmacovigilance.- Consumers' specially protected data that are necessary for the pharmacovigilance activity will be collected and processed pursuant to regulations on data protection and pharmacovigilance.

7. Data security.

General principle.- The party responsible for the file and, if applicable, the party in charge of processing must implement the technical and organisational measures necessary to guarantee the security of the personal data and prevent their alteration, loss, unauthorised processing or unauthorised access, taking into account the state of technology, the nature of the data stored and the risks to which the data are exposed, whether due to human action or to the physical or natural environment.

Clinical research.- Sponsors that have decided not to apply the dissociation procedure provided by the Action Protocol on Clinical Trials and other Clinical Researches, and sponsors that, despite having applied this procedure, have become aware of the subject's identity, will apply high-level security measures, provided the subject's identification data are not cancelled. These measures will not apply in the event that the laboratory has decided to work with dissociated data.

Pharmacovigilance.- Pharmacovigilance Units of laboratories that have adhered to this Standard Code may apply the high-level security measures. These measures will not apply in the event that the laboratory has decided to work with dissociated data.

A laboratory that, despite having dissociated the data, has become aware of the consumer's identity, will apply high-level security measures, provided the consumer's identification data are not cancelled.

8. Duty of secrecy.

General principle.- The party responsible for the file and the persons involved in any phase of personal data processing are required to maintain professional secrecy in relation to the data and to safeguard the data. These obligations will remain in effect even after the end of their relations with the file owner or, if applicable, the party responsible for the file.

Clinical research.- All clinical research personnel of the laboratories, pharma companies and CROs adhered to this Standard Code will have a duty of secrecy with respect to the personal data accessed and will sign a confidentiality clause.

Pharmacovigilance.- All the Pharmacovigilance Unit personnel of the laboratories adhered to this Standard Code will have a duty of secrecy with respect to the personal data accessed and will sign a confidentiality clause.

9.- Disclosure of Data.

General principle.- The personal data processed may only be disclosed to a third party for purposes directly related to the assignor's and the assignee's legitimate functions, and with the interested party's prior consent. Consent will be void for the disclosure of personal data to a third party when the information provided to the interested party does not indicate the intended use of the data the disclosure of which is authorised or the type of activity of the party to which the data are to be disclosed.

Consent to the disclosure of personal data is also revocable. The party to which the personal data are disclosed is required to observe the provisions of the LOPD.

Clinical research.- When the subject's informed consent is obtained, the situations in which the sponsor may disclose the subject's personal data to a third party will be explained. Such cases must be directly related to the clinical research in progress.

The subject's consent will not be necessary in the following cases:

a) Where the assignment is authorised by law.

b) Where the assignment of personal health data is necessary to resolve an emergency requiring access to a file or to conduct epidemiological studies in the terms of State and regional healthcare legislation.

Sponsors that apply the dissociation procedure provided by the Action Protocol on Clinical Trials and other Clinical Researches may assign the dissociated data as deemed fit.

Pharmacovigilance.- The subject's consent must be obtained to disclose his or her personal data to a third party.

Laboratories that process consumers' personal data in dissociated form, applying the provisions of the Pharmacovigilance Action Protocol, may assign the dissociated data as deemed fit.

10.- Access and Processing for the Account of Third Parties.

General principle.- Third-party access to the data will not constitute data disclosure when access is necessary to provide a service to the party responsible for the file.

The processing of data for the account of third parties must be regulated by an agreement that must be written or in another form that allows its existence and content to be evidenced, stipulating the following minimum obligations:

- Obligation of the party in charge of processing to process the data solely in accordance with the instructions of the party responsible for the file.
- Obligation to treat the personal data accessed under the agreement in the strictest confidence.
- Obligation of the party in charge of processing not to apply or use the data for any purpose other than the one stated in the agreement, nor to disclose the data to other parties, not even for preservation purposes.
- Security measures that the party in charge of processing is required to implement during data treatment for the account of third parties.
- Obligation not to store the data in handheld devices or to process the data outside the laboratory's facilities.
- Obligation of the party in charge of processing to destroy or return the data to the party responsible for the file when the provision of services has ended.

In the event that the party in charge of processing uses the data for any other purpose, discloses the data or uses the data in breach of contract, it will also be held responsible for processing and will be liable for any infringements personally committed.

Clinical research.- In any event, services contracted to third parties with access to data will be governed by the contractual regime provided by Article 12 LOPD and Articles 20 et seq of Royal Decree 1720/2007, of 21 December 2007, whereby the Enabling Regulations for Organic Law 15/1999, of 13 December 1999, on Personal Data Protection (RLOPD) were approved.

Pharmacovigilance.- Laboratories that contract services to third parties with access to data must in any event apply the contractual regime contained in Article 12 LOPD and Articles 20 et seq RLOPD.

11.- Data Preservation.

General principle.- The personal data must be cancelled when they are no longer necessary or relevant to the purpose for which they were collected or registered.

The personal data will be stored in a manner that allows the exercise of the right of access, unless they are legally cancelled.

Clinical research.- Sponsors that have decided not to apply the dissociation procedure provided in the Action Protocol on Clinical Trials and other Clinical Researches and sponsors that, despite having applied this procedure, have become aware of the subject's identity, must in any event dissociate the data that they decide to keep, following the end of the period that applicable regulations and industry practices deem necessary for the fulfilment of the investigation objectives. The dissociation procedure applied must guarantee the elimination of any piece of data that allows the subject's identity to be determined.

Pharmacovigilance.- Laboratories must, in any event, dissociate the data that they decide to keep, following the end of the period that applicable regulations and industry practices deem necessary for the fulfilment of the pharmacovigilance objectives. The dissociation procedure applied must guarantee the elimination of any piece of data that allows the consumer's identity to be determined.

III. ACTION PROTOCOL FOR THE EXERCISE OF RIGHTS OF ACCESS, RECTIFICATION, CANCELLATION AND OPPOSITION IN PHARMACOVIGILANCE AND CLINICAL RESEARCH USING PERSONAL DATA AND DISSOCIATED DATA

1.- Introduction And Scope Of Application.

The rights of access, rectification, cancellation and opposition (***"ARCO rights"***, as referred to in the introduction section of this protocol) are the rights specifically stipulated in data protection regulations that empower interested parties to access, rectify, cancel or object to their data, following the legally established procedure that is developed in this Action Protocol.

The Standard Code uses, without distinction, the term interested party or affected party to refer to the individual owner of the data that are processed.

For the purpose explained above, this Action Protocol establishes the guidelines to be followed by laboratories with pharmacovigilance units and by the parties involved in a Clinical Research who are responsible for processing requests to exercise ARCO rights.

This Action Protocol is divided into five large sections on (2) general considerations; (3) pharmacovigilance using personal data; (4) pharmacovigilance using dissociated data; (5) clinical research using personal data; and (6) clinical research using dissociated data.

Attached at the end of this Action Protocol, as **Annex I**, are a number of illustrative model letters for interested parties wishing to exercise any of the rights described in this protocol. Also attached as Annexes to this protocol are illustrative model letters to be sent to interested parties who have exercised these rights or, if applicable, have revoked their consent to the processing of their data.

Pursuant to Article 6 of Royal Decree 1720/2007, of 21 December 2007, whereby the Enabling Regulations for Organic Law 15/1999, of 13 December 1999, on Personal Data Protection are approved (RLOPD, as indicated above), it should be noted that where a period of days is stated, only business days will be counted, and where the period is expressed in months, it will run from date to date.

2.- General Considerations.

Having defined the scope of this Action Protocol, each of the ARCO rights must be defined in order to understand the terminology used in this protocol:

- Right of access: This is the affected party's right to obtain information on whether or not his or her own personal data are being processed, the purpose of the processing, if applicable, and the information available on the source of the data and disclosures of the data already completed or planned. Processing means any technical operation or procedure, automated or otherwise, that allows the collection, recording, preservation, preparation, modification, consultation, utilisation, cancellation, blocking or suppression of the data, and the assignment of the data as a result of notifications, consultations, interconnections and transfers.
- Right of rectification: The interested party's right to have data that are inaccurate or incomplete modified.
- Right of cancellation: Power to request the suppression of data that are inaccurate, inadequate or excessive, without affecting the blocking duty stipulated in the RLOPD.
- Right of opposition: The interested party's right to prevent the processing of his or her personal data or to order the discontinuance of processing in certain cases.

Right to access files and to rectify, cancel and object to data are highly personal rights and will be exercised by the interested party vis-à-vis the party responsible for the file. The interested party must therefore demonstrate his or her identity to the party responsible. However, the interested party's legal representative may act where the interested party is disabled or is a minor and may not personally exercise these rights.

Having identified the content of the ARCO rights, the following general considerations applicable to all the rights should be noted:

1. ARCO rights are independent rights, such that any interested party may exercise any of the rights, without the exercise of one of the rights being a pre-requisite to exercise another of the rights.
2. The interested party must be provided with a simple and cost-free means of exercising the ARCO rights. Cases in which the party responsible for the file or for processing stipulates that the interested party may exercise the rights by sending registered letters or through similar means, using telecommunication services that entail an additional cost or any other means that generate excessive cost for the interested party will not be deemed to fulfil the provisions of the RLOPD.
3. Where there are customer care or claims services, the interested party may be granted the possibility of exercising ARCO rights through those services. In this case, the interested party's identity will be deemed to be evidenced through the ordinary mechanisms in place to identify customers when providing services or contracting products.
4. ARCO rights may be exercised by interested parties by electronic mail, provided identification is adequately assured, and the party responsible for the file or processing may ask the interested party for supplementary information to ensure correct identification.
5. Request requirements.

The rights must be exercised by sending a letter to the party responsible for the file or processing, including the following details:

a. Interested party's full name.

b. Photocopy of his or her national ID card, passport or other valid ID document and, if applicable, of the ID document of the representative, or equivalent electronic instruments; and the document or electronic instrument attesting to such representation. The use of an electronic ID signature will exclude the need to present photocopies of the national ID card or equivalent document.

c. Request being made.

d. Address for notices; date and requesting party's signature.

e. Documents supporting the request, if applicable.

6. If the request does not fulfil the requirements specified in the preceding point, the party responsible for the file or processing must ask the requesting party to correct them, granting a 10-day correction period.

7. The request submitted by the subject participating in a clinical research or by the person that reports an adverse event to a pharmacovigilance unit must be answered in any event, whether or not the interested party's personal data are in the files of the party that receives the request.

As soon as a request is received from an interested party (generally in the form of a letter), the department that manages the file containing the interested party's data must be immediately informed.

In any event, the department personnel must be familiar with the general concepts of data protection for the exercise of ARCO rights by interested parties and with the ordinary procedure to be followed to comply with the LOPD and its enabling regulations, particularly the RLOPD.

3.- Pharmacovigilance Using Personal Data.

In the event that the laboratory has decided not to apply the dissociation procedure stipulated in Section II of the Pharmacovigilance Action Protocol, it will hold identification data and health data of the product consumer and, if applicable, identification data of a reporter other than the consumer.

Consequently, the pharmaceutical laboratory that has the Pharmacovigilance Unit is the party responsible for the file containing those data.

Set out below is a description of the way in which the laboratory must respond to requests to exercise each of the interested party's rights.

A. Right of Access

The affected party is entitled to obtain information on whether or not his or her own personal data are being processed, the purpose of the processing, if applicable, and the information available on the source of the data and

disclosures of the data already completed or planned. This right may be exercised in intervals of not less than twelve months, unless the interested party demonstrates a legitimate reason.

Request requirements

a) Request sent to the party responsible for the file, through any means that guarantees the identification of the interested party (ID card, electronic signature or other analogous means) and, if applicable, the identification of the representative together with the document attesting to representative status.

b) The request must state the address for notices, the date and the requesting party's signature, and it must be accompanied by a photocopy of his or her ID card.

c) Barring particularly complex cases, the interested party may refer in the consultation both to specific data and data included in a specific file, or to all the data processed by the party responsible for the file.

Means of communication

a) The interested party must be provided with a simple and cost-free means of exercising the right of access, which may not include registered letters or means that entail an excessive cost for the interested party.

b) Where the laboratory has a customer care service, the interested party may be granted the possibility of exercising the right of access through that service, in which case the interested party will be identified through the ordinary mechanisms in place to identify customers when providing services or contracting products.

c) The right of access may be exercised by interested parties by electronic mail, provided identification is adequately assured, and the laboratory may ask the interested party for supplementary information to ensure correct identification.

What must the party responsible for the file or processing (laboratory) do?

a) When an access request is received, the person that first receives the request must take note of the date of receipt and also check the period during which a reply must be sent. Subsequently, the request must be sent to the department responsible for processing matters related to data protection. The request will be resolved within a maximum of one month as from receipt.

b) The laboratory, as the party responsible for the file, must reply to the request received, whether or not the interested party's personal data are included in its files, using any means that generates evidence of the content of the reply and the date of receipt, e.g. notarised document, telegram or bureau fax with acknowledgement of receipt and registered content, and any other means deemed valid by law, provided evidence of the interested party's receipt of the document is obtained.

Attached as **Annex II** to this protocol is a model letter for the reply to the interested party in the event that his or her data are not included in the laboratory's files.

In the event that the request does not fulfil the above-mentioned requirements, the laboratory must ask the interested party to correct the request, granting a 10-day correction period.

c) Where the request has been examined and fulfils the requirements described, and the right of access has not been granted together with the reply to the interested party's request, access must be granted within ten days as from notification.

Attached as **Annex III** to this protocol is a model letter for the laboratory to reply to the interested party's request to exercise the right of access.

d) The file consultation systems to be used to allow the interested party to exercise the right of access are as follows:

1. On-screen viewing.
2. Document, copy or photocopy sent by registered or ordinary mail.
3. Fax.
4. E-mail or other electronic communication systems.
5. Any other system offered by the party in charge of processing based on the material configuration of the file or the nature of the processing.

Depending on the material configuration of the file or the nature of the processing, consultation systems may be restricted provided the system offered is cost-free. In any event, the interested party may demand a written notification.

The laboratory, as the party responsible for the file, must have in place the security measures stipulated in the RLOPD when access is provided.

The interested party may reject the system offered by the party responsible in order to allow access, even though the system is adequate. In such cases, the laboratory will not be answerable either for potential security risks affecting the information or for costs associated with the system chosen by the interested party to exercise his or her right of access.

e) Access may only be denied where the right has already been exercised during a 12-month period prior to the request and by virtue of a legal provision. If access is denied, the interested party must be informed of his or her right to request protection from the Spanish Data Protection Agency.

f) The information that must be provided by the party responsible for the file will include the interested party's basic data and the data resulting from any preparation or processing of the basic data, the source of the data, disclosures of the data already completed or planned, and details of the specific uses and purposes for which the data will be stored. The information will be provided in a perfectly understandable manner, without using codes that require the use of specific mechanical devices.

g) Moreover, where the Pharmacovigilance Unit is partially or fully formed by personnel employed by a CRO contracted by the laboratory, and the right of access is exercised vis-à-vis the CRO, the CRO must first take note of when the request is received and then immediately forward it to the laboratory so that a reply may be issued on a timely basis to guarantee the exercise of the right. Attached as **Annex IV** to this protocol is an illustrative model letter for the reply to the interested party, stating that the request has been forwarded to the party responsible for the file, in this case the laboratory.

B. Rights of Rectification and Cancellation

These rights consist of the interested party's power to demand that the party responsible for the file fulfils the obligation to ensure that the data are accurate, rectifying or cancelling personal data that are incomplete or inaccurate, or inadequate or excessive, if applicable, where the processing is not lawful.

Nonetheless, the personal data must be duly blocked during the periods stipulated in the Document on Pharmacovigilance Good Practices.

Where the data rectified or cancelled have previously been assigned, the party responsible for the file must notify the assignee of the rectification or cancellation within 10 days.

Request requirements

a) Request sent to the party responsible for the file, through any means that guarantees the identification of the interested party (ID card, electronic signature or other analogous means) and, if applicable, the identification of the representative together with the document attesting to representative status.

b) The request must state the address for notices, the date and the requesting party's signature, and it must be accompanied by a photocopy of his or her ID card.

c) The rectification or cancellation request must state the data to which it refers and the correction or cancellation to be made. It must be accompanied by documentation supporting the requested rectification, unless this depends solely on the interested party's consent.

Means of communication

a) The interested party must be provided with a simple and cost-free means of exercising the rights of rectification and cancellation, which may not include registered letters or means that entail an excessive cost for the interested party.

b) Where the laboratory has a customer care service, the interested party may be granted the possibility of exercising the rights of rectification and cancellation through that service, in which case the interested party will be

identified through the ordinary mechanisms in place to identify customers when providing services or contracting products.

c) The rights of rectification and cancellation may be exercised by interested parties by electronic mail, provided identification is adequately assured, and the laboratory may ask the interested party for supplementary information to ensure correct identification.

What must the party responsible for the file or processing (laboratory) do?

a) As explained previously, the person that first receives the request must take note of the date of receipt and also check the period during which a reply must be sent. Subsequently, the request must be sent to the department responsible for processing matters related to data protection.

b) Rectification and/or cancellation will be completed within a maximum of one month as from receipt of the request.

c) If the data have previously been assigned, the laboratory, as the party responsible for the file, must notify the assignee of the exercise by the interested party of the right of rectification or cancellation, within a 10-day period, and the assignee must rectify or cancel the data also within a 10-day period. However, the interested party need not be notified of the rectification or cancellation by the assignee.

d) The laboratory must reply to the request in any event, whether or not the interested party's personal data are included in its files, using any means that generates evidence of the content of the reply and the date of receipt, e.g. notarised document, telegram or bureau fax with acknowledgement of receipt and registered content, and any other means deemed valid by law, provided evidence of the interested party's receipt of the document is obtained.

   Attached as **Annex II** to this protocol is a model letter for the reply to the interested party in the event that his or her data are not included in the laboratory's files.

   Moreover, in the event that the request does not fulfil the necessary requirements, the laboratory must ask the interested party to correct the request, granting a 10-day correction period.

e) Cancellation entails the blocking of the data (by means, for example, of a logical mark that precludes any kind of processing), which are then only available to Public Administrations, Judges and Courts in connection with potential liabilities arising from the processing of the data, during the relevant lapsing periods (serious infringements of the LOPD lapse after three years). The lapsing periods of other offences, such as tax offences (four years), or any other obligations imposed by other regulations must be considered.

f) When may rectification and cancellation be denied?

The data must be preserved for the period stipulated in each case by applicable legislation. It may also be denied where stipulated in a provision of law.

In any event, if the exercise of the rights of rectification or cancellation is denied, the interested party must be informed of his or her right to seek protection from the Spanish Data Protection Agency or, if applicable, Spain's regional authorities.

g) The law requires the rectification or cancellation of personal data that have not been processed in accordance with the LOPD, particularly when the data are incomplete or inaccurate.

h) Finally, in cases in which the Pharmacovigilance Unit is partially or fully formed by personnel employed by a CRO contracted by the laboratory, and the right of rectification or cancellation is exercised vis-à-vis the CRO, the CRO must first take note of when the request is received and then immediately forward it to the laboratory so that a reply may be issued on a timely basis to guarantee the exercise of the right. Attached as **Annex IV** to this protocol is an illustrative model letter for the reply to the interested party, stating that the request has been forwarded to the party responsible for the file, in this case the laboratory.

Annexs V and VI contain, respectively, model replies to be used by the laboratory as the party responsible for the file when requests to exercise the rights of rectification and cancellation are received from interested parties.

C. Right of Opposition

The right of opposition is the interested party's right to prevent the processing of his or her personal data or to order the discontinuance of processing in certain cases.

Request requirements

a) Request sent to the party responsible for the file, through any means that guarantees the identification of the interested party (ID card, electronic signature or other analogous means) and, if applicable, the identification of the representative together with the document attesting to representative status.

b) The request must state the address for notices, the date and the requesting party's signature, and it must be accompanied by a photocopy of his or her ID card.

c) If opposition relates to a case in which the interested party's consent is not necessary for the processing of his or her data, the interested party must state in the request the well-founded and legitimate reasons supporting the exercise of the right of opposition.

Means of communication

a) The interested party must be provided with a simple and cost-free means of exercising the right of opposition, which may not include registered letters or means that entail an excessive cost for the interested party.

b) Where the laboratory has a customer care service, the interested party may be granted the possibility of exercising the right of opposition through that service, in which case the interested party will be identified through the ordinary mechanisms in place to identify customers when providing services or contracting products.

c) The right of opposition may be exercised by interested parties by electronic mail, provided identification is adequately assured, and the laboratory may ask the interested party for supplementary information to ensure correct identification.

What must the party responsible for the file or processing (laboratory) do?

a) As with the above-mentioned rights, the person that first receives the request must take note of the date of receipt and also check the period during which a reply must be sent. Subsequently, the request must be sent to the department responsible for processing matters related to data protection.

b) The laboratory, as the party responsible for the file, must reply to the request received within 10 days of receipt, whether or not the interested party's personal data are included in its files, using any means that generates evidence of the content of the reply and the date of receipt, e.g. notarised document, telegram or bureau fax with acknowledgement of receipt and registered content, and any other means deemed valid by law, provided evidence of the interested party's receipt of the document is obtained.

   Attached as **Annex II** to this protocol is a model letter for the reply to the interested party in the event that his or her data are not included in the laboratory's files.

   In the event that the request does not fulfil the above-mentioned requirements, the laboratory must ask the interested party to correct the request within 10 days.

   Finally, the laboratory also has a 10-day period within which to reject the interested party's request.

c) In cases in which the Pharmacovigilance Unit is partially or fully formed by personnel employed by a CRO contracted by the laboratory, and the right of opposition is exercised vis-à-vis the CRO, the CRO must first take note of when the request is received and then immediately forward it to the laboratory so that a reply may be issued on a timely basis to guarantee the exercise of the right. Attached as **Annex IV** to this protocol is an illustrative model letter for the reply to the interested party, stating that the request has

been forwarded to the party responsible for the file, in this case the laboratory.

Annex VII contains a model reply to be used by the laboratory when requests to exercise the right of opposition are received from interested parties.

D. Revocation of consent.

In general, personal data processing requires the interested party's unequivocal consent, although Article 6 LOPD provides a number of exceptions to this general rule.

The interested party has the right to revoke the consent initially given to the processing of his or her data. As in previous cases, revocation of consent does not affect the duty of the party responsible for the file to block the interested party's personal data in case of potential liabilities arising from the processing of the data or to keep the data available to Public Administrations, Judges and Courts.

The interested party may revoke consent using a cost-free means that does not generate income for the party responsible for the file. In particular, adequate means recognised for the revocation of consent are a pre-franked letter sent to the party responsible for the file or a call to a laboratory's customer care service. As in the previous cases, the interested party may not be required to send a registered letter or to use means that entail the payment of an additional price or an excessive cost.

What must the party responsible for the file or processing (laboratory) do?

The person that first receives the request must take note of the date of receipt and also check the period during which a reply must be sent. Subsequently, the request must be sent to the department responsible for processing matters related to data protection.

The laboratory, as the party responsible for the file, must cease to process the interested party's data within 10 days. If the interested party wishes, the laboratory must specifically confirm that data processing has actually been discontinued.

If the data have previously been assigned, the laboratory, as the party responsible for the file, must notify the assignees of the revocation of consent so that they also discontinue the processing of the interested party's personal data.

In cases in which the Pharmacovigilance Unit is partially or fully formed by personnel employed by a CRO contracted by the laboratory, and the right of revocation is exercised vis-à-vis the CRO, the CRO must first take note of when the request is received and then immediately forward it to the laboratory so that a reply may be issued on a timely basis to guarantee the exercise of the right of revocation. Attached as **Annex IV** to this protocol is an illustrative model letter for the reply to the interested party, stating that the request has been forwarded to the party responsible for the file, in this case the laboratory.

Attached as **Annex VII** to this protocol is a model letter for the laboratory, as the party responsible for the file, to confirm to the interested party that the processing of his or her personal data has been discontinued as requested.

4.- Pharmacovigilance Using Dissociated Data.

In the event that the laboratory has applied the dissociation procedure stipulated in Section II of the Pharmacovigilance Action Protocol, it will not hold in its files the identification data and health data of the product consumer or, if applicable, the identification data of a reporter other than the consumer.

However, the laboratory could have collected personal data of other parties (suppliers, employees, etc.) and must therefore first check that the request to exercise ARCO rights does not relate to the data contained in any of those other files.

As indicated previously, the laboratory is required to reply to the interested party's request whether or not his or her data are included in the laboratory's files.

In the event of a request, the laboratory must therefore reply to the interested party stating that it holds no personal data in its files and that the request cannot be fulfilled.

Annex II contains a model letter for the laboratory to inform the interested party of the absence of personal data.

5.- Clinical Research Using Personal Data.

As stipulated in the Action Protocol on Clinical Trials and other Clinical Researches, clinical research projects using personal data include two separate files for which different parties are responsible.

These two files are described below, indicating the party responsible for the file in each case:

Clinical Investigation File (CIF). This is the file of the Healthcare Centre at which the investigation is conducted. The file comprises all the subject's clinical documentation and the data generated in relation to the study. These data are processed for general study management purposes. The party responsible for the CIF is (are) the centre(s) at which the study is undertaken.

Case Report Form File (CRFF). This is the file of the laboratory (trial sponsor). It comprises all the information required to conduct the study, in accordance with the study protocol. The purpose of processing the CRFF data is to evaluate the study results and draw conclusions. The party responsible for the CRFF is the study sponsor.

The centre, as the party responsible for the CIF, must allow affected parties to exercise their ARCO rights as stipulated in the LOPD and the RLOPD.

With respect to the CRFF, the laboratory, as the study sponsor, must allow interested parties to exercise their rights.

It should be noted that in cases in which the sponsoring laboratory has contracted to a third party (e.g. a CRO) the execution of certain functions requiring access to the CRFF, that third party must first take note of when the request is received and must then immediately forward it to the department responsible for matters related to data protection at the sponsoring laboratory so that a reply may be issued on a timely basis to guarantee the exercise of the right.

A. Right of Access

This is the affected party's right to obtain information on whether or not his or her own personal data are being processed, the purpose of the processing, if applicable, and the information available on the source of the data and disclosures of the data already completed or planned.

This right may be exercised in intervals of not less than twelve months, unless the interested party demonstrates a legitimate reason.

Request requirements

a) Request sent to the party responsible for the file, through any means that guarantees the identification of the interested party (ID card, electronic signature or other analogous means) and, if applicable, the identification of the representative together with the document attesting to representative status.

b) The request must state the address for notices, the date and the requesting party's signature, and it must be accompanied by a photocopy of his or her ID card.

c) Barring particularly complex cases, the interested party may refer in the consultation both to specific data and data included in a specific file, or to all the data processed by the party responsible for the file.

Means of communication

a) The interested party must be provided with a simple and cost-free means of exercising the right of access, which may not include registered letters or means that entail an excessive cost for the interested party.

b) Where the laboratory has a customer care service, the interested party may be granted the possibility of exercising the right of access through that service, in which case the interested party will be identified through the ordinary mechanisms in place to identify customers when providing services or contracting products.

c) The right of access may be exercised by interested parties by electronic mail, provided identification is adequately assured, and the laboratory may ask the interested party for supplementary information to ensure correct identification.

What must the party responsible for the file or processing (sponsoring laboratory) do?

a) The person that first receives the request must take note of the date of receipt and also check the period during which a reply must be sent. Subsequently, the request must be sent to the department responsible for processing matters related to data protection.

b) When a request is received, the sponsoring laboratory or its representative in Spain, as the party responsible for the CRFF, must reply within one month as from receipt of the request. To this end, given the brevity of the deadline and the significance of the penalties if it is not met, the department must determine when the interested party's notification arrived and through what means (post, e-mail, etc.), and must calculate the reply deadline, ensuring that the provisions of law and the provisions contained in each of the sections of this protocol are observed.

c) The sponsoring laboratory, as the party responsible for the CRFF, must reply to the request received, whether or not the interested party's personal data are included in its files, using any means that generates evidence of the content of the reply and the date of receipt, e.g. notarised document, telegram or bureau fax with acknowledgement of receipt and registered content, and any other means deemed valid by law, provided evidence of the interested party's receipt of the document is obtained.

   Attached as **Annex II** to this protocol is a model letter for the reply to the interested party in the event that his or her data are not included in the sponsoring laboratory's files.

   In the event that the request does not fulfil the above-mentioned requirements, the sponsoring laboratory must ask the interested party to correct the request, granting a 10-day correction period.

d) Where the request has been examined and fulfils the requirements described, and the right of access has not been granted together with the reply to the interested party's request, access must be granted within ten days as from notification.

   Attached as **Annex III** to this protocol is a model letter for the sponsoring laboratory to reply to the interested party's request to exercise the right of access.

e) The file consultation systems to be used to allow the interested party to exercise the right of access are as follows:

   1. On-screen viewing.
   2. Document, copy or photocopy sent by registered or ordinary mail.
   3. Fax.
   4. E-mail or other electronic communication systems.

5. Any other system offered by the party in charge of processing based on the material configuration of the file or the nature of the processing.

Depending on the material configuration of the file or the nature of the processing, consultation systems may be restricted provided the system offered is cost-free. In any event, the interested party may demand a written notification.

The sponsoring laboratory, as the party responsible for the CRFF, must have in place the security measures stipulated in the RLOPD when access is provided.

The interested party may reject the system offered by the party responsible in order to allow access, even though the system is adequate. In such cases, the sponsoring laboratory will not be answerable either for potential security risks affecting the information or for costs associated with the system chosen by the interested party to exercise his or her right of access.

f) Access may only be denied where the right has already been exercised during a 12-month period prior to the request and by virtue of a legal provision. If access is denied, the interested party must be informed of his or her right to request protection from the Spanish Data Protection Agency.

g) The information that must be provided by the sponsoring laboratory, as the party responsible for the CRFF, will include the interested party's basic data and the data resulting from any preparation or processing of the basic data, the source of the data, disclosures of the data already completed or planned, and details of the specific uses and purposes for which the data will be stored. The information will be provided in a perfectly understandable manner, without using codes that require the use of specific mechanical devices.

h) In cases in which the sponsoring laboratory has contracted to a third party (e.g. a CRO) the execution of certain functions requiring access to the CRFF, that third party must first take note of when the request is received and must then immediately forward it to the department responsible for matters related to data protection at the sponsoring laboratory so that a reply may be issued on a timely basis to guarantee the exercise of the right. Attached as **Annex IV** to this protocol is an illustrative model letter for the reply to the interested party, stating that the request has been forwarded to the party responsible for the file, in this case the sponsoring laboratory.

B. <u>Rights of Rectification and Cancellation</u>.

These rights consist of the interested party's power to demand that the party responsible for the file fulfils the obligation to ensure that the data are accurate, rectifying or cancelling personal data that are incomplete or inaccurate, or inadequate or excessive, if applicable, where the processing is not lawful.

Nonetheless, the personal data must be duly blocked during the periods stipulated in Royal Decree 1345/2007, of 11 October 2007, whereby the procedure for the authorisation, registration and dispensation of industrially-

manufactured medicinal products for human use was introduced, and Order SCO/256/2007, of 5 February 2007, establishing the principles and detailed guidelines of good clinical practice and the requirements for authorising the manufacture or import of investigational medicinal products for human use.

Where the data rectified or cancelled have previously been assigned, the party responsible for the file must notify the assignee of the rectification or cancellation within 10 days.

Request requirements

a) Request sent to the party responsible for the file, through any means that guarantees the identification of the interested party (ID card, electronic signature or other analogous means) and, if applicable, the identification of the representative together with the document attesting to representative status. The request will state the data that must be cancelled or rectified.

b) The request must state the address for notices, the date and the requesting party's signature, and it must be accompanied by a photocopy of his or her ID card.

c) The rectification or cancellation request must state the data to which it refers and the correction or cancellation to be made. It must be accompanied by documentation supporting the requested rectification, unless this depends solely on the interested party's consent.

Means of communication

a) The interested party must be provided with a simple and cost-free means of exercising the rights of rectification and cancellation, which may not include registered letters or means that entail an excessive cost for the interested party.

b) Where the sponsoring laboratory has a customer care service, the interested party may be granted the possibility of exercising the rights of rectification and cancellation through that service, in which case the interested party will be identified through the ordinary mechanisms in place to identify customers when providing services or contracting products.

c) The rights of rectification and cancellation may be exercised by interested parties by electronic mail, provided identification is adequately assured, and the laboratory may ask the interested party for supplementary information to ensure correct identification.

What must the party responsible for the file or processing (sponsoring laboratory) do?

a) As explained previously, the person that first receives the request must take note of the date of receipt and also check the period during which a reply

must be sent. Subsequently, the request must be sent to the department responsible for processing matters related to data protection.

b) Rectification and/or cancellation will be completed within a maximum of one month as from receipt of the request.

c) If the data have previously been assigned, the sponsoring laboratory, as the party responsible for the CRFF, must notify the assignee of the exercise by the interested party of the right of rectification or cancellation, within a 10-day period, and the assignee must rectify or cancel the data also within a 10-day period. However, the interested party need not be notified of the rectification or cancellation by the assignee.

d) The sponsoring laboratory must reply to the request in any event, whether or not the interested party's personal data are included in its files, using any means that generates evidence of the content of the reply and the date of receipt, e.g. notarised document, telegram or bureau fax with acknowledgement of receipt and registered content, and any other means deemed valid by law, provided evidence of the interested party's receipt of the document is obtained.

   Attached as **Annex II** to this protocol is a model letter for the reply to the interested party in the event that his or her data are not included in the sponsoring laboratory's files.

   Moreover, in the event that the request does not fulfil the necessary requirements, the sponsoring laboratory must ask the interested party to correct the request, granting a 10-day correction period.

e) Cancellation entails the blocking of the data (by means, for example, of a logical mark that precludes any kind of processing), which are then only available to Public Administrations, Judges and Courts in connection with potential liabilities arising from the processing of the data, during the relevant lapsing periods (serious infringements of the LOPD lapse after three years). The lapsing periods of other offences, such as tax offences (four years), or any other obligations imposed by other regulations must be considered.

f) When may rectification and cancellation be denied?

   The data must be preserved for the period stipulated in each case by applicable legislation. It may also be denied where stipulated in a provision of law.

   In any event, if the exercise of the rights of rectification or cancellation is denied, the interested party must be informed of his or her right to seek protection from the Spanish Data Protection Agency or, if applicable, Spain's regional authorities.

g) The law requires the rectification or cancellation of personal data that have not been processed in accordance with the LOPD, particularly when the data are incomplete or inaccurate.

h) In cases in which the sponsoring laboratory has contracted to a third party (e.g. a CRO) the execution of certain functions requiring access to the CRFF,

the third party must first take note of when the request is received and then immediately forward it to the department responsible for matters related to data protection at the sponsoring laboratory, so that a reply may be issued on a timely basis to guarantee the exercise of the right. Attached as **Annex IV** to this protocol is an illustrative model letter for the reply to the interested party, stating that the request has been forwarded to the party responsible for the file, in this case the sponsoring laboratory.

Annexes V and VI contain, respectively, model replies to be used by the laboratory as the party responsible for the file when requests to exercise the rights of rectification and cancellation are received from interested parties.

C. Right of Opposition

The right of opposition is the interested party's right to prevent the processing of his or her personal data or to order the discontinuance of processing in certain cases.

Request requirements

a) Request sent to the party responsible for the file, through any means that guarantees the identification of the interested party (ID card, electronic signature or other analogous means) and, if applicable, the identification of the representative together with the document attesting to representative status.

b) The request must state the address for notices, the date and the requesting party's signature, and it must be accompanied by a photocopy of his or her ID card.

c) If opposition relates to a case in which the interested party's consent is not necessary for the processing of his or her data, the interested party must state in the request the well-founded and legitimate reasons supporting the exercise of the right of opposition.

Means of communication

a) The interested party must be provided with a simple and cost-free means of exercising the right of opposition, which may not include registered letters or means that entail an excessive cost for the interested party.

b) Where the laboratory has a customer care service, the interested party may be granted the possibility of exercising the right of opposition through that service, in which case the interested party will be identified through the ordinary mechanisms in place to identify customers when providing services or contracting products.

c) The right of opposition may be exercised by interested parties by electronic mail, provided identification is adequately assured, and the laboratory may

ask the interested party for supplementary information to ensure correct identification.

What must the party responsible for the file or processing (sponsoring laboratory) do?

a) As with the above-mentioned rights, the person that first receives the request must take note of the date of receipt and also check the period during which a reply must be sent. Subsequently, the request must be sent to the department responsible for processing matters related to data protection.

b) The sponsoring laboratory, as the party responsible for the file, must reply to the request received within 10 days of receipt, whether or not the interested party's personal data are included in its files, using any means that generates evidence of the content of the reply and the date of receipt, e.g. notarised document, telegram or bureau fax with acknowledgement of receipt and registered content, and any other means deemed valid by law, provided evidence of the interested party's receipt of the document is obtained.

   Attached as **Annex II** to this protocol is a model letter for the reply to the interested party in the event that his or her data are not included in the sponsoring laboratory's files.

   In the event that the request does not fulfil the above-mentioned requirements, the party responsible for the file must ask the interested party to correct the request within 10 days.

   Finally, the sponsoring laboratory also has a 10-day period within which to reject the interested party's request.

c) In cases in which the sponsoring laboratory has contracted to a third party (e.g. a CRO) the execution of certain functions requiring access to the CRFF, the third party must first take note of when the request is received and then immediately forward it to the department responsible for matters related to data protection at the sponsoring laboratory, so that a reply may be issued on a timely basis to guarantee the exercise of the right. Attached as **Annex IV** to this protocol is an illustrative model letter for the reply to the interested party, stating that the request has been forwarded to the party responsible for the file, in this case the sponsoring laboratory.

Annex VII contains a model reply to be used by the laboratory when requests to exercise the right of opposition are received from interested parties.

D. <u>Revocation of Consent</u>

In general, personal data processing requires the interested party's unequivocal consent, although Article 6 LOPD provides a number of exceptions to this general rule.

The interested party has the right to revoke the consent initially given to the processing of his or her data. As in previous cases, revocation of consent does

not affect the duty of the party responsible for the file to block the interested party's personal data in case of potential liabilities arising from the processing of the data or to keep the data available to Public Administrations, Judges and Courts.

The interested party may revoke consent using a cost-free means that does not generate income for the party responsible for the file. In particular, adequate means recognised for the revocation of consent are a pre-franked letter sent to the party responsible for the file or a call to a laboratory's customer care service. As in the previous cases, the interested party may not be required to send a registered letter or to use means that entail the payment of an additional price or an excessive cost.

What must the party responsible for the file or processing (sponsoring laboratory) do?

The person that first receives the request must take note of the date of receipt and also check the period during which a reply must be sent. Subsequently, the request must be sent to the department responsible for processing matters related to data protection.

The sponsoring laboratory, as the party responsible for the CRFF, must cease to process the interested party's data within 10 days. If the interested party wishes, the sponsoring laboratory must specifically confirm that data processing has actually been discontinued, using any means that generates evidence of the content of the reply and the date of receipt, e.g. notarised document, telegram or bureau fax with acknowledgement of receipt and registered content, and any other means deemed valid by law, provided evidence of the interested party's receipt of the document is obtained.

If the data have previously been assigned, the sponsoring laboratory, as the party responsible for the CRFF, must notify the assignees of the revocation of consent so that they also discontinue the processing of the interested party's personal data.

In cases in which the sponsoring laboratory has contracted to a third party (e.g. a CRO) the execution of certain functions requiring access to the CRFF, the third party must first take note of when the request is received and then immediately forward it to the department responsible for matters related to data protection at the sponsoring laboratory, so that a reply may be issued on a timely basis to guarantee the exercise of the right. Attached as **Annex IV** to this protocol is an illustrative model letter for the reply to the interested party, stating that the request has been forwarded to the party responsible for the file, in this case the sponsoring laboratory.

Attached as **Annex VII** to this protocol is a model letter for the sponsoring laboratory, as the party responsible for the CRFF, to confirm to the interested party that the processing of his or her personal data has been discontinued as requested.

6.- Clinical Research Using Dissociated Data.

As stipulated in the Action Protocol on Clinical Trials and other Clinical Researches, the party responsible for the file in clinical researches using dissociated data is the centre at which the study is conducted.

In the case of multi-centre researches, all the centres involved are responsible for their files.

The centre, as the party responsible for the clinical investigation file (CIF), must respond to requests to exercise ARCO rights received from affected parties, pursuant to the LOPD and RLOPD.

The sponsor is the party responsible for processing the CIF because, although it does not access the personal data on the subjects involved in the study, the sponsor establishes the data processing criteria.

Consequently, although the sponsor is not required to reply to requests to exercise ARCO rights, set out below are certain precautions that must be observed in the event that an interested party sends a request to exercise ARCO rights to the sponsor.

As the sponsor does not hold the interested parties' identification data, the sponsor may not in any event forward the request to exercise ARCO rights to the centre (party responsible for the CIF) and may not inform the interested party which centre is the party responsible for the CIF in each clinical study for which the sponsor is responsible.

However, the sponsor may hold personal data of other parties (suppliers, employees, etc.) and must therefore first check that the request to exercise ARCO rights does not refer to data contained in any of these other files.

Having verified this, the sponsor must inform the interested party that none of his or her data is included in the sponsor's files. The sponsor must also inform the interested party that, if he or she has participated in any other clinical investigation project, the request to exercise ARCO rights must be sent to the party responsible for the CIF, which will be the centre at which the study in which the interested party participated is taking place or took place.

Annex II contains a model letter to be used by the sponsor to reply to requests from interested parties to exercise ARCO rights.

ANNEX I

Exercise of the Affected Party's Rights

Exercise of the right of access

PARTICULARS OF THE PARTY RESPONSIBLE FOR THE FILE OR PROCESSING

PARTICULARS OF THE REQUESTING PARTY

Mr/Ms _____, of full age, whose address is c/_____, No. _____, town _____, province _____, postcode _____, holding national ID number _____, a photocopy of which is attached, hereby declares that he/she wishes to exercise the right of access, pursuant to Article 15 of Organic Law 15/1999 and Articles 27 to 30 of Royal Decree 1720/2007, of 21 December 2007, whereby the Enabling Regulations were introduced for Organic Law 15/1999, of 13 December 1999, on Personal Data Protection.

REQUEST

1.- Please provide me with access to my files, at no cost, within a maximum period of one month as from receipt of this request.

2.- Should this request to exercise my right of access be accepted, please send the information by post to the address stated above within ten days as from the decision to accept the access request.

3.- The information should contain my basic personal data that are included in your files and the results of any preparation, processing or treatment, indicating the source of the data, the assignees and details of the specific uses and purposes for which my data are stored, in a legible and intelligible form.

In _____, on _____ (month) _____ 20___

Signature: _____

The content of this Annex must be adapted to each specific case.

ANNEX I (continuation)

Exercise of the Affected Party's Rights

Exercise of the right of rectification

PARTICULARS OF THE PARTY RESPONSIBLE FOR THE FILE OR PROCESSING

PARTICULARS OF THE REQUESTING PARTY

Mr/Ms _____, of full age, whose address is c/_____, No. _____, town _____, province _____, postcode _____, holding national ID number _____, a photocopy of which is attached, hereby declares that he/she wishes to exercise the right of rectification, pursuant to Article 16 of Organic Law 15/1999 and Articles 31 to 33 of Royal Decree 1720/2007, of 21 December 2007, whereby the Enabling Regulations were introduced for Organic Law 15/1999, of 13 December 1999, on Personal Data Protection.

REQUEST

1.- Please correct the incorrect data relating to my person included in your files, at no cost, within ten days as from receipt of this request.

2.- The data to be rectified are listed on a sheet attached to this document, referring to the documents that accompany this request as evidence, if necessary, of the accuracy of the new data.

3.- Please notify me in writing when the data have been rectified, at the address stated above.

4.- In the event that the party responsible for the file considers that rectification is not admissible, please notify me of this decision and the reasons within that ten-day period, so that I may lodge the claim envisaged in Article 18 of Organic Law 15/1999, of 13 December 1999, on Personal Data Protection.

In _____, on _____ (month) _____ 20___

Signature:_____

The content of this Annex must be adapted to each specific case.

ANNEX I (continuation)

Exercise of the Affected Party's Rights

Exercise of the right of cancellation

PARTICULARS OF THE PARTY RESPONSIBLE FOR THE FILE OR PROCESSING

PARTICULARS OF THE REQUESTING PARTY

Mr/Ms _____, of full age, whose address is c/_____, No. _____, town _____, province _____, postcode _____, holding national ID number _____, a photocopy of which is attached, hereby declares that he/she wishes to exercise the right of cancellation, pursuant to Article 16 of Organic Law 15/1999 and Articles 31 to 33 of Royal Decree 1720/2007, of 21 December 2007, whereby the Enabling Regulations were introduced for Organic Law 15/1999, of 13 December 1999, on Personal Data Protection.

REQUEST

1.- Please cancel any data relating to my person that are included in your files, within ten days as from receipt of this request, as stipulated in Organic Law 15/1999, of 13 December 1999, on Personal Data Protection, and notify me in writing at the address stated above.

2.- In the event that the party responsible for the file considers that cancellation is not admissible, please notify me of this decision and the reasons within that ten-day period, so that I may lodge the claim envisaged in Article 18 of Organic Law 15/1999, of 13 December 1999, on Personal Data Protection.

In _____, on _____ (month) _____ 20___

Signature:_____

The content of this Annex must be adapted to each specific case.

ANNEX I (continuation)

Exercise of the Affected Party's Rights

Exercise of the right of opposition

PARTICULARS OF THE PARTY RESPONSIBLE FOR THE FILE OR PROCESSING

PARTICULARS OF THE REQUESTING PARTY

Mr/Ms _____, of full age, whose address is c/_____, No. _____, town _____, province _____, postcode _____, holding national ID number _____, a photocopy of which is attached, hereby declares that he/she wishes to exercise the right of opposition, pursuant to Article 6, subsection 4 of Organic Law 15/1999 and Articles 34 to 36 of Royal Decree 1720/2007, of 21 December 2007, whereby the Enabling Regulations were introduced for Organic Law 15/1999, of 13 December 1999, on Personal Data Protection.

REQUEST

1.- Please exclude the data relating to my person that are included in your files, within ten days as from receipt of this request, due to the existence of well-founded and legitimate reasons arising from specific personal circumstances.

2.- The data to be excluded are listed on a sheet attached to this document, referring to the documents that accompany this request as evidence of my reasons, if necessary.

3.- Please notify me in writing when the data have been excluded, at the address stated above.

4.- In the event that the party responsible for the file considers that opposition to the processing of these data is not admissible, please notify me of this decision and the reasons within that ten-day period.

In _____, on _____ (month) _____ 20____

Signature:_____

The content of this Annex must be adapted to each specific case.

ANNEX II

Model Letter Informing of the Absence of Personal Data

In _____, on _____ (month) _____ 200_ [maximum of 10 days as from receipt of the letter]

Mr / Ms _____
_____
_____

Dear Sir / Madam,

Further to your request, and pursuant to Organic Law 15/1999, of 13 December, 1999 on Personal Data Protection and Article 25.2 of Royal Decree 1720/2007, of 21 December 2007, whereby the Enabling Regulations were introduced for Organic Law 15/1999, of 13 December 1999, on Personal Data Protection, I write in my capacity as the representative of [……] (hereinafter […]), whose address is _____, to certify the following matters:

I- In reply to your request, we confirm that this entity's files contain no personal data relating to your person or to your representative.

II- **(This point is only applicable to Clinical Researches)** In the event that you or your representative have participated in any clinical research and you wish to exercise the rights of access, rectification, cancellation or opposition in connection with the personal data relating to your person or to your representative, you must direct contact the Healthcare Centre at which the research was conducted, which is the Party responsible for the File.

Yours faithfully,

Mr/Ms _____

The content of this Annex must be adapted to each specific case.

ANNEX III

Model Reply to a Request to Exercise the Right of Access

In _____, on _____ (month) _____ 20___

Mr / Ms _____
_____
_____

Dear Sir / Madam,

Further to your request, and pursuant to Organic Law 15/1999, of 13 December 1999, on Personal Data Protection, Article 15 of which guarantees the right of access, I write in my capacity as the representative of [.....] (hereinafter [...]), whose address is _____, to certify the following matters:

I.- In reply to your request, we inform you that the following personal data relating to your person are included in the personal data file of [.....], entered in the Data Protection Agency's General Register of Personal Data:

_____
_____

II.- Additionally, and as requested by you, we provide you with the following information:

Your data were obtained from: [1] _____
_____

[1] State the source of the data, i.e. the way in which the subject provided his/her data to the relevant Agent/Party.

Your data have been provided to:[2] _____
_____

[2] Identity of the individual or legal entity to which the interested party's data have been assigned, provided any data have been assigned.

Your personal data were stored in order to [3] _____
_____

[3] Specify the uses and purposes for which the data were stored].

III.- We have replied to your request to exercise the right of access in conformity with Article 15 of Organic Law 15/1999, of 13 December 1999, on Personal Data Protection and applicable enabling regulations.

Accordingly, and as [...] wishes to allow you to exercise your rights in full, we inform you that we are at your entire disposal should you require any clarifications.

Yours faithfully,

Mr/Ms _____

The content of this Annex must be adapted to each specific case.

ANNEX IV

Model Reply to a Request to Exercise the Rights of Access, Rectification, Cancellation, Opposition and Revocation of Consent (Party in charge of processing)

In _____, on _____ (month) _____ 20____

Mr / Ms _____
_____
_____

Dear Sir / Madam,

Further to your request, and pursuant to Organic Law 15/1999, of 13 December 1999, on Personal Data Protection and Article 25.2 of Royal Decree 1720/2007, of 21 December 2007, whereby the Enabling Regulations were introduced for Organic Law 15/1999, of 13 December 1999, on Personal Data Protection, I write in my capacity as the representative of [……] (hereinafter […]), whose address is _____, to certify the following matters:

I- In accordance with prevailing legislation, your request has been forwarded to the Party responsible for the File containing your personal data or those of your representative. In this case, the Party responsible for the File is [……], whose address is [……]

II- As the party ultimately responsible for replying to requests to exercise the rights of access, rectification, cancellation or opposition (as applicable) received from interested parties, the Party responsible for the File must take a decision on this process and notify you accordingly.

Despite the content of point II, and as […] wishes to allow you to exercise your rights in full, we inform you that we are at your entire disposal should you require any clarifications.

Yours faithfully,

Mr/Ms _____

The content of this Annex must be adapted to each specific case.

ANNEX V

Model Reply to a Request to Exercise the Right of Rectification

In _____, on _____ (month) _____ 20____

Mr / Ms _____
_____
_____

Dear Sir / Madam,

Thank you for your request to rectify your personal data.

In reply to your request, I write in my capacity as the representative of [.....] (hereinafter [...]), whose address is _____, to certify the following matters:

I.- As requested, we have rectified your personal data included in the personal data file of [.....] entered in the Data Protection Agency's General Register of Personal Data.

II.- Your personal data contained in the file, following rectification, are as follows: _____

_____

_____

III.- Your personal data have been rectified in conformity with Article 16 of Organic Law 15/1999, of 13 December 1999, on Personal Data Protection and applicable enabling regulations.

Yours faithfully,

Mr/Ms _____

The content of this Annex must be adapted to each specific case.

ANNEX VI

Model Reply to a Request to Exercise the Right of Cancellation

In _____, on _____ (month) _____ 20____

Mr / Ms _____
_____
_____

Dear Sir / Madam,

Further to your request, and pursuant to Organic Law 15/1999, of 13 December 1999, on Personal Data Protection, I write in my capacity as the representative of [.....] (hereinafter [...]), whose address is _____, to certify the following matters:

I.- As requested, we have cancelled your personal data included in the personal data file of [.....] entered in the Data Protection Agency's General Register of Personal Data under code number: _____

II.- The following personal data have been cancelled:

_____
_____

III.- Your personal data have been cancelled in conformity with Article 16 of Organic Law 15/1999, of 13 December 1999, on Personal Data Protection and applicable enabling regulations.

Accordingly, and as our Company wishes to fulfil your request in full, we inform you that this will be our final contact with you, notwithstanding any letter that has already been issued.

Yours faithfully,

Mr/Ms _____

The content of this Annex must be adapted to each specific case.

ANNEX VII

Model Confirmation of the Discontinuance of Personal Data Processing (Rights of opposition and revocation)

In _____, on _____ (month) _____ 20____

Mr / Ms _____
_____
_____

Dear Sir / Madam,

Further to your request, and pursuant to Organic Law 15/1999, of 13 December 1999, on Personal Data Protection and its enabling regulations, I write in my capacity as the representative of [……..] (hereinafter […]), whose address is _____, to certify the following matters:

I.- As requested by you, we confirm that as from the date of this letter the processing of your personal data included in the personal data file of […..] entered in the Data Protection Agency's General Register of Personal Data has been discontinued:

_____.

II.- The personal data the processing of which has been discontinued are as follows:
_____
_____

III.- The processing of your personal data has been discontinued in conformity with Article 17 of the Enabling Regulations for Organic Law 15/1999, of 13 December 1999, on Personal Data Protection, introduced under Royal Decree 1720/2007.

Accordingly, and as our Company wishes to fulfil your request in full, we inform you that henceforth your personal data will not be processed by the Company and that, consequently, this will be our final contact with you, notwithstanding any letter that has already been issued.

Yours faithfully,

Mr/Ms _____

The content of this Annex must be adapted to each specific case.

5.4. ACTION PROTOCOL ON THE SELF-REGULATION SYSTEM

I.- Introduction and scope of application

II.- Standard Code Steering Committee

III.- Complaint resolution proceeding

IV.- Follow-up obligations

Annex I: Complaint form to be sent to Farmaindustria's Standard Code Steering Committee

I. INTRODUCTION AND SCOPE OF APPLICATION.

The purpose of this Action Protocol is to establish the procedure for the supervision by Farmaindustria of compliance with the obligations contained in the Standard Code (the Standard Code being the consolidated text and the action protocols described in it), in relation to both clinical research and pharmacovigilance.

The scope of the procedure described here encompasses laboratories or pharmaceutical companies and CROs (Contract Research Organisations) adhered to the Code.

This document contains the follow-up and review systems for the application and development of the Standard Code, in addition to establishing means of communicating with the Spanish Personal Data Protection Agency (AEPD).

In accordance with Article 6 of Royal Decree 1720/2007, of 21 December 2007, whereby the Enabling Regulations for Organic Law 15/1999, of 13 December 1999, on Personal Data Protection were introduced (RLOPD), it should be noted that where a period of days is stated, only business days will be counted, and where the period is expressed in months, it will run from date to date.

II. STANDARD CODE STEERING COMMITTEE.

Composition

The Standard Code Steering Committee shall be designated by Farmaindustria's Governing Board at the proposal of the Governing Council. Committee members shall hold office for four years. The Committee shall be composed of:

a) Three members, all of whom shall be technicians or professionals of recognized prestige, and shall be fully independent from the laboratories and CROs.

b) A Secretariat designated from among Farmaindustria's Legal Department, who shall assist the members and be entitled to attend at Committee meetings, express his opinion but has no vote.

Independence

In the event that a member of the Steering Committee detects a conflict of interests with the laboratory or the CRO against which the complaint has been presented, or should the laboratory or CRO detect a conflict of interests, the member must refrain from participating in the examination of the complaint and immediately notify the Governing Board.

The Governing Board, *ex officio* or at the request of any of its members, will analyse the conflict of interests raised and, if appropriate, shall designate a new member to replace the challenged member, solely and exclusively to examine the proceeding relating to the complaint presented.

During the period of incompatibility, the challenged member may not have access to the proceeding file.

Functions

The Committee shall ensure the effective fulfilment of the Standard Code and the observance of the rights of the interested parties who lodge complaints.

In addition to its functions as the body responsible for examining complaints proceedings and claims, and for imposing penalties, the Committee shall have the following functions:

a) Monitor the application of the Standard Code, proposing any amendments deemed fit to Farmaindustria's Governing Board;

b) Coordinate the dissemination, promotion, interpretation, fulfilment and any other aspects of the Standard Code, keeping the AEPD up to date with the application of the Code, pursuant to section IV of this Action Protocol.

c) Analyse and accept or reject requests to adhere to this Standard Code, update the list of laboratories and CROs adhered to the Standard Code, and submit the information to the AEPD, pursuant to section IV of this Action Protocol.

d) Any other function that may be necessary or advisable for the correct application of the Standard Code.

Meetings

Ordinary meetings of the Committee shall be held on a quarterly basis and, in particular, when a complaint has been received for an infringement of the obligations described in the Standard Code. Decisions shall be taken by majority of the members, whose deliberations shall be secret. Minutes of such meetings shall be prepared to be signed by the Committee Secretariat and members, and recorded in a minute's book.

Authority

Without prejudice to the AEPD's authority to impose penalties, the Standard Code Steering Committee shall have the authority to initiate, examine and resolve the procedure on complaints received in connection with this Standard Code.

III. COMPLAINT RESOLUTION PROCEEDING.

In general, and under Article 3.e) of Organic Law 15/1999, of 13 December 1999, on Personal Data Protection (LOPD), the affected party or interested party is the individual owner of the data that are processed. Data processing means any technical operation or procedure, automated or otherwise, that allows the collection, recording, preservation, preparation, modification, blocking and cancellation of data, as well as data assignments resulting from notifications, consultations, interconnections and transfers.

The complaint resolution proceeding is stipulated without prejudice to the AEPD's powers to impose penalties under the LOPD and the right of the affected parties to obtain the AEPD's protection.

All affected parties that become aware of activities of a laboratory or CRO infringing the Standard Code, the LOPD or the RLOPD will be entitled to present a complaint.

The complaint right may be exercised, firstly, before the laboratory or CRO allegedly responsible for the infringement, by sending a letter to its headquarters within 15 days as from the date on which the action to be rectified is known, using means that generate evidence of the date of receipt of the letter.

The laboratory or CRO will have a maximum of one month as from the date of receipt of the complaint to correct the alleged infringement.

If the laboratory or CRO has not corrected the infringement that gave rise to the complaint by the end of that period, the affected party may fill in the form attached as **ANNEX I** to this Action Protocol and send it to Farmaindustria's headquarters, to the attention of the Standard Code Steering Committee. Additionally, the complaint may also be presented through Farmaindustria's website http://www.farmaindustria.es, in the section Standard code/complaints. In both cases, the deadline will be 15 days and the evidence of the alleged infringement held by the affected party must be submitted.

Where the affected party sends the complaint directly to Farmaindustria, it will be forwarded to the laboratory or CRO against which the complaint is made in order for the infringement to be rectified within one month, provided it relates to a laboratory adhered to the Standard Code. Otherwise, Farmaindustria will forward the complaint to the AEPD. If the reported conduct is not rectified, or when Farmaindustria deems fit, due to the content of the complaint, a complaint resolution proceeding will be initiated.

Before initiating the proceeding, if the Standard Code Steering Committee becomes aware that the complaint presented to it is at the same time the object of a complaint or claim already presented to the AEPD, it will shelve the proceeding and notify the AEPD and the parties involved accordingly. However, both parties (the AEPD and the Standard Code Steering Committee) will maintain fluid communication in relation to all matters affecting the complaint and any other aspects deemed fit.

Proceeding

The complaint resolution proceeding will consist of three phases:

a) Activities of the Steering Committee to precisely determine the facts giving rise to the complaint.

b) Allegations phase in which the interested parties may submit any documents and information deemed fit. In turn, the Standard Code Steering Committee may gather any evidence deemed necessary.

c) Once the allegations and evidence gathering phase has ended, the Steering Committee will adopt a decision and notify the interested parties accordingly.

Infringements

Infringements will be classed as minor, serious or very serious.

Minor infringements:

a) Failure to complete, or cancel and replace, *ex officio*, for formal reasons, the personal data of subjects participating in clinical research projects or of consumers/legal representatives or other reporters who have experienced or reported an adverse event, when they are known to be incorrect or incomplete.

b) Failure to inform the subject participating in a clinical research project, the consumer or the consumer's legal representative or other reporter, of the provisions of this Code governing clinical research and pharmacovigilance.

c) Failure to conclude, with a CRO or any other individual or legal entity with access to data during the provision of a service, a data processing assignment contract in accordance with the provisions of this Code governing clinical research and pharmacovigilance.

Serious infringements:

a) Collection and processing of the personal data of subjects participating in a clinical research project without their consent, or of consumers, legal representatives or other reporters that contact the pharmacovigilance service without the consent of the person or the legal representative; in pharmacovigilance, where such consent is necessary.

b) Processing of the personal data of subjects participating in a clinical research project without their consent, or of consumers, legal representatives or other reporters that contact the pharmacovigilance service for purposes (commercial, promotional, etc.) that are incompatible with the ones for which the data were collected.

c) In the context of a clinical research project, obtainment of specially protected personal data from information sources other than the subject participating in the clinical research project, his or her legal representative or the investigator.

d) Prevention or hindering of the exercise of the rights of access, rectification, cancellation and opposition, or the refusal to provide the information requested.

e) Failure to eliminate data or to dissociate data after the end of the period during which they may be stored under applicable sector regulations, as necessary to fulfil the clinical research or research objectives.

f) When working with dissociated data, processing of personal data that have not previously been dissociated of subjects participating in clinical research projects or of consumers, legal representatives or other reporters that contact the pharmacovigilance services, together with evaluations, comments, statistics, conclusions or any other piece of data.

g) Interference with the independence of the persons responsible for dissociation, in relation to a clinical research project or pharmacovigilance activities.

h) Where the data are not dissociated, access by unauthorised personnel to areas containing the identification data of subjects participating in the clinical research or of consumers, legal representatives or other reporters that contact the pharmacovigilance service.

i) When, in the context of a clinical research project in which the data are dissociated, a numerical or alphanumerical code is assigned that permits the identification of the subject participating in the clinical research project.

j) When the data are dissociated, failure to implement the necessary preventive measures to avoid access to identification data in the context of clinical research and pharmacovigilance.

k) Registration of the consumer's identification data when, in pharmacovigilance activities, the decision has been taken to dissociate consumers' data.

l) Where, in pharmacovigilance activities using dissociated data, the identification data of consumers, legal representatives or other reporters are included in notifications sent.

Very serious infringements:

a) Collection and processing of specially protected personal data without the specific consent of the subject participating in a clinical research project, or the consumer that contacts the pharmacovigilance service; in pharmacovigilance, where such consent is necessary.

b) International assignment or transfer of personal data of a subject participating in a clinical research or a consumer that contacts the pharmacovigilance service without the subject's consent or the necessary authorisation from the Director of the Spanish Data Protection Agency, where necessary.

c) Failure to observe the duty of secrecy in both clinical research and pharmacovigilance activities.

e) Notifications or assignments of data where this is not permitted.

Penalties

The penalties that may be imposed by the Standard Code Control Body, without affecting the AEPD's powers to impose penalties, are as follows:

a) Penalties for minor infringements: written warning.

b) Penalties for serious infringements: written warning and temporary suspension of adherence to the Standard Code until the correction of the infringement has been verified.

c) Penalties for very serious infringements: written warning and temporary or, if applicable, definitive suspension of adherence to the Standard Code, depending on the seriousness of the infringement.

Each of the penalties envisaged will entail the obligation to correct the defects or irregularities observed and to rectify inadequate situations or conduct.

IV. FOLLOW-UP OBLIGATIONS.

Obligations following the registration of the Standard Code.

Farmaindustria will ensure that up-to-date information on the laboratories and CROs adhered to the Standard Code, the content of the Code, adherence procedures and compliance guarantees are publicly accessible.

This information will be available in Farmaindustria's website: http://www.farmaindustria.es in the Standard Code section and will be clear and concise.

Farmaindustria undertakes to favour access by all persons, placing particular emphasis on disabled and elderly persons.

Farmaindustria will prepare an Annual Report that will be submitted to the AEPD, containing the following points:

a) Activities carried out to disseminate the Standard Code and to promote adherence to the Code.

b) Activities conducted to verify compliance with the Standard Code and findings.

c) Complaints and claims processed and outcome.

d) Up-to-date list of the laboratories and CROs adhered to the Standard Code.

e) Any other aspect that should be highlighted.

Farmaindustria will evaluate the effectiveness of the Standard Code at least every four years. In this evaluation, Farmaindustria will measure the level of satisfaction of the laboratories and CROs adhered, and of the affected parties, and will propose updates to the content of the Standard Code to bring it into line with data protection regulations applicable from time to time.

Amendments to this Standard Code will be submitted to the AEPD for review and approval.

ANNEX I

COMPLAINT FORM TO BE SENT TO FARMAINDUSTRIA'S STANDARD CODE STEERING COMMITTEE

COMPLAINT TO FARMAINDUSTRIA'S STANDARD CODE STEERING COMMITTEE

AFFECTED PARTY'S DATA (1)

Mr/Ms ....., of full age, whose address is ..... No. ....., Town ..... Province ..... Postcode ..... Region of Spain ..... holding national ID number .....

DATA OF THE LABORATORY/CRO (2)

Name / company name: Mr/Ms ..... (on behalf of and representing .....) ....., whose address is .... No. ..... Postcode ..... Town ..... Province ..... Region of Spain ..... holding tax code .....

Pursuant to section III of this Action Protocol, on the complaint resolution proceeding, the Standard Code Steering Committee is hereby notified of the following facts, which are supported by the documentation attached to this form:

FACTS

ONE: ..... (supported by attached document number ....).
TWO: ..... (supported by attached document number ....).
THREE: ..... (supported by attached document number ....).

Accordingly,

IT IS REQUESTED that the complaint against the entity identified in this document be acknowledged and processed as envisaged in the applicable provisions of Farmaindustria's Standard Code.

In ....., on ..... (month) 2xxx

Signed:

COMITÉ DE SEGUIMIENTO DEL CÓDIGO TIPO DE FARMAINDUSTRIA
(FARMAINDUSTRIA'S STANDARD CODE STEERING COMMITTEE)
Serrano, 116
28006 Madrid

---

1 The complaint may be presented by the affected party, in which case a copy of his or her national ID card or other legally admissible document attesting to his or her identity must be submitted. Legal representation may be granted to a third party, in which case the national ID card and proxy document must also be submitted.
2 In the case of a legal entity, the document indicating the individual that is the entity's legal representative must be submitted.

The content of this Annex must be adapted to each specific case.

6

ADHERENCE AND ACCREDITATION SYSTEM

6. ADHERENCE AND AC CREDITATION SYSTEM.

ADHERENCE AND ACCREDITATION SYSTEM

6.1 Application to adhere to the Code

Companies (laboratories that may or may not be members of Farmaindustria and CRO) wishing to adhere to this Standard Code must fulfil the obligations imposed by data protection regulations and declare files containing personal data to the AEPD, as an adherence pre-requisite.

They must also submit a written request to adhere to the Standard Code in which they specifically agree to fulfil the obligations stipulated in the Code.

Attached at the end of this Standard Code, as **Annex I**, is an illustrative model application to adhere to the Standard Code, which will be sent to the Steering Committee for analysis and approval.

6.2 Confirmation of adherence to the Code

The Steering Committee must issue a specific decision within a maximum of three months as from receipt of all the supplementary and additional documentation that may be requested together with the application, accepting or rejecting adherence to the Standard Code. In the event of rejection, the reasons must be indicated, as well as the way in which any errors or weaknesses may be corrected.

6.3 List of entities adhered to the Code

The list of entities adhered to the Standard Code is publicly available and may be consulted in Farmaindustria's website http://www.farmaindustria.es, in the Standard Code section.

Farmaindustria undertakes to keep this list permanently up to date and to inform the AEPD of any addition, removal or change to the list.

6.4 Accreditation

Having regard to clinical research, the sponsor will state both in the trial protocol and in the other trial documentation its adherence to the Standard Code and compliance with the data protection obligations imposed.

With respect to pharmacovigilance, the laboratory will state both in the consent document, where consent is necessary, and in the rest of the documentation its adherence to the Standard Code and compliance with the data protection obligations imposed.

ANNEX I

APPLICATION TO ADHERE TO THE CODE

Applicant company	
Address	
Postcode	
Town	
Tax code	
Farmaindustria member	YES NO

Mr/Ms ....., holding national ID number ....., on behalf of and representing the above-mentioned company, wishes to adhere to Farmaindustria's Standard Code on Personal Data Protection in connection with clinical research and pharmacovigilance, registered at the Spanish Data Protection Agency by means of the decision dated .....

The company also declares that it fulfils the conditions stipulated in this Standard Code and accepts and submits to all the provisions of the Code in relation to personal data protection.

With respect to the processing of data in clinical researches, the applicant states that it selects the option marked below with an x:

- ☐ The dissociation procedure stipulated in this Standard Code will be applied.
- ☐ Patients' identification data will be processed and the files will be registered at the General Data Protection Agency.
- ☐ No clinical researches are conducted.

Having regard to the pharmacovigilance service, the applicant states that it selects the option marked below with an x:

- ☐ The dissociation procedure stipulated in this Standard Code will be applied.
- ☐ Patients' identification data will be processed and the files will be registered at the General Data Protection Agency.
- ☐ No pharmacovigilance activities are conducted.

Accordingly,

the applicant requests that the Standard Code Steering Committee acknowledge the submission of this application to adhere to the Standard Code and approve its adherence to the Code.

In witness whereof, and for all pertinent purposes, I sign this document in ....., on ..... (month) ..... 2xxx.

Signed:

7

TRAINING

TRAINING.

- Entities adhered to this Standard Code must arrange data protection training for the personnel and professionals that process personal data.

- Farmaindustria will conduct training activities consisting of annual seminars in which general data protection issues will be addressed. Nonetheless, when new regulations are published or specific issues are raised by entities adhered to our Standard Code, Farmaindustria will organise *ad hoc* seminars to address the specific data protection issues raised.

- Personal data training activities will be more detailed and frequent for laboratory professionals who, given the nature and functions of their post and/or due to the area of the internal organisation of which they form part, could have a more direct relationship with the affected parties and their data.

  The professionals that could more frequently access or process personal data include the persons referred to below:

  a) Personnel from the Clinical Research Department, particularly personnel responsible for verifying the accuracy of the content of case report forms.

  b) Pharmacovigilance service personnel.

  c) Personnel responsible for the audits performed on clinical research projects and on source documents used by Pharmacovigilance Units.

  d) External Pharmacovigilance Unit personnel.

  e) Legal departments (particularly in connection with the exercise of the rights of access, rectification, cancellation and opposition).

- Farmaindustria will inform the entities adhered to this Standard Code, on a timely basis, of all data protection training sessions that may be of interest to them.