ABHI Code of Conduct for the Medical Device Industry on the Processing of Personal Data

1st September 2004
# Table of Contents

I  INTRODUCTION .................................................................................................................................3

III  ABHI CODE OF CONDUCT .................................................................................................................................6

IV  ADMINISTRATION OF THE CODE ..................................................................................................................7

Section 1:  Scope ..................................................................................................................................................8

Section 2:  Key Principles ..................................................................................................................................9

Section 3:  Data Privacy Officer ..........................................................................................................................11

Section 4:  Consent for the Processing of Personal Data .........................................................................................12

Section 5:  Information to be Given to the Data Subject participating in a Clinical Investigation ..............14

Section 6:  Data Subject’s Right of Access to Personal Data .................................................................................15

Section 7:  Secondary Data Processing ..............................................................................................................16

Section 8:  Adverse Events and Corrective Action ...............................................................................................17

Section 9:  Security of Processing .......................................................................................................................19

Section 10:  Transborder Data Flow ..................................................................................................................20

Section 11:  Quality Control, Quality Assurance .................................................................................................21

Section 12:  Summary of Regulatory Activities involving Personal Data .............................................................22
I  INTRODUCTION

The European Council and Parliament Directive 95/46/EC (1) on ‘the protection of individuals with regard to the processing of personal data and on the free movement of such data’ (the “Directive”) as enacted in the UK by means of the Data Protection Act 1998 (the “Regulation”) has a direct impact on the operation of the medical devices industry, including scientific research activities, investigation of adverse events and the supply of custom-made products. While the bulk of this Code focuses on Clinical Investigations, it is also intended to cover other legitimate industry activities - particularly those mandated by Medical Devices legislation - and reference to these issues is made below.

Legitimate concerns about protecting privacy can and should be met in a manner that encourages innovative research, improves patient care, and enables the medical device industry to meet its statutory and ethical obligations. The Association of British Health-Care Industries (ABHI)¹ is conscious of the need to create an environment favourable for the medical device industry to develop new devices for the public benefit whilst at the same time protecting individual privacy.

The medical device industry already takes steps to ensure the confidentiality, integrity and availability of personal data in a manner that preserves the fundamental rights of data subjects. Safeguards are to a large extent enshrined in the existing regulatory and legislative framework governing international medical device research and development. Wherever reasonably practicable, and subject to exceptions provided by Data Protection laws, obtaining consent prior to the processing of personal data is central to acknowledging and establishing the rights of individuals to privacy.

ABHI fully supports the enactment of personal data protection rules and regulations proposed in the Regulation. However, care must be taken so that the Regulation is implemented in such a way that legitimate research and regulatory responsibilities will not be adversely affected or impeded.

The introduction of legislation on personal data protection should balance the need to protect individual privacy and the need to improve health through the continuing discovery and evaluation of innovative medical devices by considering that scientific research carried out within the medical devices industry represents a ‘substantial public interest’.

ABHI has therefore adopted this ‘Code of Conduct for the Medical Devices Industry on the Processing of Personal Data’ (hereafter referred to as the ‘Code’) which is intended to complement the Regulation and provide guidance to the medical device industry in the UK.

This Code has been drafted in consultation with the Information Commissioner.

In this Code of Conduct, reference is made to “consent”. Consent may be explicit where a person expressly gives permission or implicit when such consent may reasonably be expected or inferred. In either case, reasonable steps should be taken when practical to inform the person concerned of the circumstances. When explicit consent is give, it is advisable (when practicable) that this be

¹ The Association of British Health-Care Industries (ABHI) is the lead trade association for the UK medical systems industry. This sector comprises not only manufacturers of medical devices, equipment and consumables, but also service companies, distributors, professional groups (such as architects and lawyers), and other suppliers to the medical community. ABHI has approximately 170 member companies whose annual output is about 80% of the industry’s total. The membership includes five Special Interest Sections and six sectoral trade associations which in turn have a further 600 member companies.
recorded in writing together with a record of the information given.
II BACKGROUND

The medical device industry makes a substantial contribution to public health by discovering, developing and optimising the delivery and use of new medical devices to prevent, diagnose and treat diseases and disabilities. Such activities are ‘of substantial public interest’ and are conducted subject to stringent safeguards designed to secure and protect the processing of personal data.

In medical device clinical research, the legitimate processing of personal data concerning health is necessary to comply with regulatory or good clinical practice (GCP) requirements and to facilitate long-term follow-up of patients and their offspring. Personal Data may also be handled in the course of other activities, many of which are statutory requirements placed on the industry. These include:

(a) Investigation of adverse events and complaints
(b) Compilation of medical databases
(c) Training and support of clinical institutions
(d) Supply of devices custom-made for individual patients
(e) Prescription supply services
(f) Supply of services such as telemedicine

Personal data concerning health may be categorised as:

(i) Directly identifiable
   Personal identifiers comprising name, address and national health (or other personal) identification number are normally sufficient to directly identify a data subject.

(ii) Indirectly identifiable
   Personal identifiers comprising one or more specific factors may be sufficient to indirectly identify a data subject. For example, an individual's initials, data of birth, age, sex, hospitalisation date, diagnosis, height and colour of eyes may be sufficient to identify a person in certain circumstances even though his or her name, address and national health (or other personal) identification number are not identified.

(iii) Not identifiable
   Personal identifiers which can directly or indirectly identify the data subject are removed or encoded and the data are retained in a form such that identification of the data subject (without access to a key to the code) is no longer possible. (This is also known as pseudonymisation).

In medical device clinical research, personal identifiers which directly identify a data subject are normally held by the treating physician (or other healthcare professional) and are not processed by medical device company personnel. In certain circumstances, however, the processing of personal data which directly identifies a data subject may be necessary or unavoidable (e.g. to permit the analysis and reporting of research data in accordance with scientific and regulatory requirements).  

Where personal data do not permit the direct or indirect identification of the data subject, such data are considered anonymous and the principles of data protection specified in the Directive do not apply (cf. Recital 26 of the Directive).

There is a legitimate need to uniquely associate data from multiple data sources with a particular data subject and from the research perspective to ensure that data are from the same patient and are aggregated correctly. This linkage can be achieved only through the use of unique personal identifiers, or possibly by combining several personal identifiers.
Individuals and society are understandably concerned about the use and safeguarding of sensitive personal information, particularly information relating to an individual’s health. ABHI shares those concerns and supports the implementation of the Regulation and the enactment by its member companies and associations of personal data protection guidance by encouraging the adoption of national codes of conduct based on this code.

The Code seeks to ensure the application of industry-wide ‘good practices’ in the processing and protection of personal data and is designed to be in compliance with the Directive. Where appropriate, the Code sets out suitable safeguards to accommodate exemptions from certain provisions of the Directive on the grounds of ‘substantial public interest’.

The Code fits into the general framework established by Article 27§1 of the Directive, whereby:

“the Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.”

The Code is also intended to encourage and foster international consistency in the implementation of national legislation by EU Member States pursuant to the Directive, taking account of the special features of the medical device sector. Adoption of national codes pursuant to the Code shall be in conformity with existing and future national laws and regulations.

The Code draws on established principles and practices laid down in various regulations and guidelines which govern the conduct of medical research and the processing of personal data, notably: the International Conference on Harmonisation (ICH); Good Clinical Practice (GCP) Consolidate Guideline (2), The International standards on clinical investigation of Medical Devices (ISO 14155) (3); The Council of Europe Recommendation on the Protection of Medical Data (4); and the OECD ‘Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data’ (5).

For convenience unless the content indicates otherwise, the acronym “GCP” is used in this Code of Practice to mean both Good Clinical Practice and the ISO Clinical Investigation Standard (references 2 and 3 above).
IV     ADMINISTRATION OF THE CODE

This Code of Conduct is a voluntary code and is addressed to ABHI's individual member companies and associations.

ABHI member companies and associations are encouraged to adopt the Code or ensure that their own practice fully reflects the principles and safeguards stated in the Code in a manner that is compatible with national laws pursuant to the Directive.

When third party organisations (e.g. contract research organisations or central laboratories) process personal data on behalf of medical device companies, the relevant ABHI company member shall be responsible for establishing SOPs and contractual arrangements with the said third parties to ensure compliance with the principles and safeguards stipulated in the Code.
Section 1: Scope

1.1 The Code covers all prospective and retrospective scientific research activities performed by the medical device industry that involve the processing of personal data on human subjects. Thus, the processing of personal data concerning patients, investigational site staff, staff employed by third party organisations and regulatory authority staff all fall within the scope of the Code.

1.2 The Code covers the following range of scientific and regulatory activities conducted by the medical device industry which are necessary to fulfil its obligations:

   a) clinical trials
   b) post-marketing clinical research and vigilance activities
   c) complaint and adverse event investigation
   d) device utilisation review and outcomes research studies
   e) health technology analysis
   f) training and education
   g) supply of custom-made devices.

1.3 The Code covers privacy issues relating to the processing of personal data for the purposes of developing and monitoring the use of new and existing medical devices products for human use. Medical devices for human use include diagnostic products to the extent that they are classified as medical devices according to applicable legislation.

1.4 The Code covers all aspects of data processing and all media (e.g. paper, electronic, etc) whether the data are collected by direct questioning or measurement, or accessed from existing databases and files.

1.5 In accordance with applicable legislation, the Code also covers privacy issues relating to access to and receipt of personal data as may be required by worldwide regulatory authorities during data audits and inspections at investigational sites, and with regards to the transfer of personal data to such authorities.

---

4 Information generated during the course of a research project may originate in different forms – paper case record form (CRF), laboratory results from the analysis of biological samples (e.g. blood, tissues), electronic data capture devices or as technical readings copied from source documents.
Section 2: Key Principles

2.1 ABHI member companies and associations will subscribe to the following principles and associated safeguards with the aim of protecting personal data while at the same time assuring the legitimate development of new medical devices and the development and surveillance of marketed products:

a) The processing of personal data in pursuit of the research, development and regulatory activities relating to medical devices must be limited to those data that are reasonably necessary to enable those activities to be carried out properly.

b) Companies must develop standard operating procedures (SOPs) to ensure that personal data are collected for a specified and legitimate purpose, are processed fairly and lawfully, are accurate, current and cover all activities involving the processing of personal data.

c) Companies must develop and conduct training programmes covering all activities associated with the processing of personal data. Such programmes will be mandatory for all staff that process personal data and will emphasise the individual’s responsibilities under the Directive and applicable national legislation.

d) Explicit consent for the processing of personal data should be obtained from the data subject (or his representative) prior to any processing operation whenever reasonably possible unless otherwise specified in the Code (cf. Sections 4 and 7), and especially during the conduct of clinical investigations.

e) In circumstances where a third party requires access to personal data but does not need to know the identity of the data subject, such access should not directly reveal the identity of the data subject.

f) Companies must provide a secure environment for the processing of personal data and should identify an individual (hereafter referred to as a “data privacy officer”) responsible for security, administration and enforcement of personal data protection policies and practice. The data privacy officer must act independently of organisational functions that process personal data. He may be an employee or an advisor of the company.

g) Company personnel whose responsibilities require access to personal data that may identify an individual must agree to keep confidential the identity of data subjects who become known to them during the course of their work.

h) Where applicable, job descriptions for all positions that involve the processing of personal data should indicate the need to ensure confidentiality. Employment contracts corresponding to such positions will include stipulations that confidentiality in data processing will be maintained.

i) Personal identifiers which directly identify a data subject shall be held, whenever possible, at the data source under the supervision of the treating physician or other official.

j) Access to personal identifiers which directly or indirectly identify a data subject will be permitted for as long as is necessary to fulfil the purpose for which the data were collected or for further processing subject (where relevant) to the safeguards specified in GCP guidelines.
k) Companies will periodically determine whether personal identifiers which directly or indirectly identify a data subject may be removed or encoded without compromising the research objective or the safety of the data subject. Whenever personal identifiers which directly identify the data subject are encoded, the Code list will be held by a trusted third party (e.g. treating physician).

l) Personal identifiers which directly identify a data subject shall be removed or encoded as soon as is possible and practical and at the latest when all legitimate processing needs have been satisfied.

m) Code lists must be maintained in a secure location and may be accessed only by approved and authorised personnel under appropriate safeguards. Access to Code lists will be controlled by a trusted third party (e.g. treating physician).

n) Whenever possible and practical, secondary processing of personal data should be conducted only after personal identifiers which directly identify the data subject have been separated. Secondary processing of personal data will be conducted subject to the same safeguards which apply to the primary processing of personal data.

o) Medical device companies which process personal data originating in another EU Member State will be responsible for ensuring that affiliates and any third party outside of the EU apply at least the same level of security of processing as governed by and implied by the Code, save to the extent that local laws and regulations provide to the contrary.

p) Companies will fully inform treating physicians, other research staff and third party organisations who process personal data of their privacy obligations under the Directive and as specified in any contractual relationships.
Section 3: Data Privacy Officer

3.1 Medical device companies are encouraged and expected to designate a data privacy officer to ensure that personal data are processed in compliance with the Code and with respect to applicable national privacy laws and regulations⁵.

3.2 The data privacy officer will be responsible for:

a) Developing and maintaining company policy and guidelines on personal data protection and data security which comply with the Regulation and which control access to personal data files; and to applicable code lists held by the company; and the handling of all requests from third parties regarding access to personal data held by the company (e.g. requests from national supervisory authorities, device regulatory authorities, treating clinicians, etc).

b) Maintaining a register of processing operations for notification to the national supervisory authority including:

- Name and address of the controller(s)
- Purpose of processing
- Description of categories of data subjects and of data relating to them
- Recipients of categories of data
- Proposed transfers of data to non-EU countries
- General description of the measures taken to ensure security of processing

c) Training and educating of company personnel with regard to data protection policies and practices.

3.3 Companies should facilitate access by complainants to their data privacy officer by making available the correct point of contact.

⁵ As stated in Article 18.2 of the Directive, the requirement to give prior notification of intended processing purposes to national supervisory authorities can be simplified or exempted if, amongst other conditions, the controller appoints a ‘data protection official’.
Section 4: Consent for the Processing of Personal Data

4.1 Whenever reasonably practicable, the explicit consent of the data subject participating in a research project must be obtained prior to the processing of personal data. However, in medical device research and regulatory activities, there are certain circumstances (see below) where obtaining consent may not be required or be practicable.

4.2.1 For data subjects participating in medical device clinical research studies conducted under GCP, an informed consent statement is the principal method whereby a data subject will give explicit consent for the processing of their personal data. Unless otherwise excluded under national laws, and subject to national provisions pursuant to the Directive, such consent will be sufficient to permit the processing of personal data. Such informed consent statement must contain all the relevant elements included in the applicable ICH GCP guidelines and ISO 14155 as well as any additional information required under applicable legal rules and regulations on personal data protection.

4.2.2 The informed consent statement should contain an assurance that methods are employed to protect personal data during all processing activities, including the transfer of data to other countries, and the potential use of data by third parties and for other acceptable purposes (e.g. publication).

4.2.3 The informed consent statement should receive the favourable opinion of a duly constituted ethics committee, and the consent of the data subject will be sought by a responsible healthcare professional prior to the processing of personal data.

4.2.4 The processing of personal data should only be permitted after the relevant consent has been obtained along with any other prior approvals required by statute or regulation.

4.3 For some legitimate medical device research projects, it may not be possible, practical or relevant to obtain the consent of the data subject prior to the processing of personal data. In these cases, a duly constituted ethics committee should agree that the research project serves a public interest and that, given the nature and purpose of the project, consent is not required. Such activities include but are not limited to:

a) Epidemiological studies
b) Studies using data on deceased patients subsequent to their participation in a research study.
c) Reporting of adverse device reactions to competent regulatory authorities in medical device regulations
d) Spontaneous adverse experience reporting (e.g. by data subjects and healthcare professionals)
e) Emergency medical protocols.

6 Informed consent is a process whereby a data subject voluntarily confirms his/her willingness to participate in a research project after having been informed about all aspects of the project that are relevant to his/her decision to participate as mentioned in national regulations and GCP.

a) The wording in the informed consent statement underlines the medical researcher’s commitment to respect applicable regulatory requirements, good clinical practice, and to comply with the ethical principles which have their origin in the Declaration of Helsinki.
b) By signing and dating the consent form, the data subject (or a legal representative) recognises the purposes of the research project, the nature of the data (including personal data) that will be collected, the processing actions that will be applied and that records identifying the data subject will be kept confidential, to the extent required by applicable laws and regulations.
In such cases, it is the responsibility of the researcher to ensure personal data are protected in accordance with the principles outlined in the Code and national legislation.

4.4 In other circumstances where personal data is processed in a manner which allows the direct identification of a data subject, informed consent should be obtained unless exempted by national laws or unless it is not reasonably practicable to do so. For example, it is not normally practicable to obtain consent from an individual lodging a complaint or from persons who may be the subject of adverse event investigations.

4.5 If the data subject is not in a position to give valid consent (e.g. is a minor, a person suffering from mental disease, etc) the informed consent of the person legally entitled to act in the interest of the data subject is required.
Section 5: Information to be Given to the Data Subject participating in a Clinical Investigation

5.1 In accordance with national legislation, information to be given to the data subject participating in a medical device research project should be provided either as part of an informed consent process or directly by the treating physician.

5.2 For prospective studies, in addition to the information provided to the data subject as specified in ICH GCP or ISO 14155, the physician, researcher or, if necessary the medical device company, will be responsible for providing to the data subject the following information consistent with the specific in study or project:

a) The identity of the Controller of the file (e.g. medical device company, affiliate)
b) Purpose of the processing activity. (e.g. This information may be used for product registration, product performance monitoring, or scientific research investigating new treatments, interventions and management procedures so that patient care outcomes are improved).
c) The recipients or categories of recipients (e.g. affiliates, contract research organisations or regulatory authorities) to whom data could be disclosed.
d) The existence of his/her right of access to and right to rectify personal data
e) The obligation of confidentiality regarding all company personnel involved in personal data processing who could either directly or indirectly identify the data subject.
f) The assurance that if the results of the research project are published, the personal data elements which could identify the data subject will remain confidential.
Section 6: Data Subject’s Right of Access to Personal Data

6.1 Data subjects will be entitled to request confirmation of the existence of personal data held by medical device companies and by their contractual partners and will have the right to rectify erroneous or inaccurate data. All such requests should be handled in accordance with the following procedures and safeguards.

a) Requests will be addressed by the Controller of the file in accordance with the provisions of national law and the technical and organisational security measures governing the processing of personal data.

b) The decision to respond to a request from a data subject should be managed in close co-operation with the treating physician or scientific investigator and the Controller of the file.

c) In most instances, disclosures of personal data to a data subject will be by, and at the discretion of, the treating physician or scientific investigator. This measure avoids the inappropriate dissemination of health data that could adversely affect the data subject’s physical or mental well being.

d) Legitimate requests from a data subject to rectify, erase or block personal data should be implemented in a timely manner unless it can be demonstrated that this would be erroneous or misleading.

e) Under certain circumstances, access to personal data may be restricted at the discretion of the treating physician or scientific investigator, specifically where access would:

   i. violate the rights of third parties whose information is contained in the data
   ii. likely seriously to disrupt an individual’s care and treatment with resultant personal harm

6.2 If it is no longer possible to directly or indirectly identify the data subject, the provisions outlined under 6.1 no longer apply.

6.3 The Act recognises that a balance needs to be maintained between the obligations to respect personal data and the need not unnecessarily to jeopardise the integrity of medical research.
Section 7 Secondary Data Processing

7.1 No further consent is required if the nature of any secondary processing falls within the scope of the purposes for which explicit consent was previously obtained.

7.2 If it is intended to further process personal data outside of the scope and purpose for which consent was previously given, then the explicit consent of the data subject should be obtained unless exempted by applicable legislation or international regulations and guidelines or:

   a) The data subject is neither directly nor indirectly identifiable from the data to be processed or,
   b) An independent third party (e.g. a properly constituted ethics committee or regulatory authority) agrees that the research project serves a public interest and that, given the nature and purpose of the project, obtaining consent is neither feasible nor practical
   c) Individual data are rendered anonymous or the data are used in an aggregated form for statistical or scientific research, and no medical risk to the data subject and no risk of breaking individual privacy rights can be foreseen.

7.3 If consent for secondary processing was included as part of the original informed consent process, the data subject will have the opportunity to withdraw his/her consent for such subsequent use on the basis of a reasonable objection and during a reasonable time period unless specifically exempted by an independent third party (e.g. a properly constituted ethics committee or regulatory authority). Secondary processing should not take place before the expiry of such reasonable period of time.
Section 8: Adverse Events and Corrective Action

8.1 Manufacturers of Medical Devices are obliged by law to investigate adverse events and to take appropriate corrective action. In certain cases, such events must be reported to the relevant authorities in the country where the event occurred. In particular, a report must be made within 30 days of the Manufacturer becoming aware of the event which could potentially have led to death or a serious injury could arise were the event to be repeated. If the event actually did lead to death or a serious injury, the report must be submitted within 10 days of the manufacturer becoming aware of the event.

8.2 Reports of adverse events are typically received from a hospital or clinician or through the Manufacturer’s own sales force or other employees. The Medical Device Regulations oblige a Manufacturer to establish systems for receiving and investigating adverse events. Increasingly, the Manufacturer is being pressured to take proactive steps to establish how his devices are performing. Such an approach is considered especially relevant for devices newly placed on the market.

8.3 In the great majority of cases, reporting and investigation of adverse events involves information about the individuals involved. Typically, the Manufacturer will learn the address of the hospital or clinic where the event took place; the nature of the event and any actual or potential harm suffered by individuals; and the names of individuals involved in the incident, be they clinicians, nurses, other clinical staff or patients. The Manufacturer may also receive medical images, e.g. radiographs or MRI scans bearing the patient’s details.

8.4 For a number of reasons, it is not normally possible either to obtain consent from each of the individuals concerned, or to ensure that they remain anonymous. Even if the latter were possible, the Manufacturer would have the key to the code, thus largely negating the benefits of anonymity.

8.5 Those persons reporting an adverse event to a Manufacturer will usually be extremely busy and/or directly involved in the adverse experience. They will not normally be prepared to sign consent forms allowing the recordal of their names. Indeed, to create a barrier, in the form of completing a consent form, is almost bound to be inimical to the effective investigation of the event.

8.6 Among the names likely to be disclosed during the investigation of an adverse event are the names of any persons who may have suffered harm. They are unlikely to sign any kind of consent form presented by a Manufacturer.

8.7 The purpose of adverse event investigation is to enable the Manufacturer (and, where relevant, the regulatory authorities) to establish the cause of the event and whether any corrective action is required. Anything which impedes that process is to be deplored, and there can be little doubt that the process would be impeded and communication made more difficult by insisting first on completion of a consent form.

8.8 It is in everyone’s interest that any corrective action is rapidly implemented. Such implementation is likely to be facilitated by knowing the names of those involved – be they clinical or administrative staff, patients or others.

8.9 Large hospitals may as a matter of course be involved in a large number of adverse events at any one time. Clarity as to the names of those involved in each incident is essential if confusion is to be avoided. Otherwise, valuable time will be lost and incorrect decisions may be made, simply because one similar incident has become confused with another.
8.10 Given the above issues, it is recommended that the Manufacturer does not impede the investigation of adverse events and implementation of corrective action by seeking to complete consent forms. Instead, the Manufacturer should regard his obligations under the Medical Devices Regulations as his prime duty. In order, so far as possible, to safeguard the privacy of individuals involved, the Manufacturer should establish procedures which safeguard the use of such personal data. The principles which should apply to such procedures are:

- Individual’s names should be revealed only to those directly involved in complaints investigation and deciding on corrective action.
- Files containing such personal data should be marked confidential and treated as such.
- No use should be put to such personal data except the investigation and corrective action process.
Section 9: Security of Processing

9.1 The processing of personal data will be subject to technical, physical and organisational security measures which ensure that:

a) An adequate level of individual data protection is achieved.

b) All legal requirements for data protection are respected and applied.

c) A mechanism is in place in the organisation concerned to handle any legitimate request or requirement from an individual to access, correct or delete personal data.

9.2 Appropriate security procedures will be applied by companies, personnel at data collection sources, data recipients and third party suppliers to all transfers of personal data amongst these parties. All parties are responsible for the security of personal data processing and must therefore establish suitable contracts with all other parties to ensure that their responsibilities are met.
Section 10: Transborder Data Flow

10.1 The transfer of personal data held by medical device companies or by third parties contracted by medical device companies to another country will be in compliance with the relevant regulations.

10.2 Intra-company transfer of personal data between one country and another country should be covered by company-specific procedures.

10.3 Transfer of personal data from a medical device company to a third party in another country will be permitted only if the organisations involved in the countries concerned have signed suitable contractual arrangements which provide all necessary safeguards to protect personal data and ensure the data subject’s rights of access.

10.4 Whenever possible, personal identifiers which may directly reveal the identity of the data subject should be removed or encoded prior to any transfer to a third party in another country.

10.5 If it is not possible or desirable to remove or encode personal identifiers which may directly or indirectly reveal the identity of the data subject prior to any transfer to a third party in another country, then the third party concerned must ensure that the processing of personal data will be carried out in a manner consistent with the Code and with regard to the scope of processing activities for which prior consent has been obtained. The level of protection afforded in the recipient country will be adequate in the opinion of the data controller in the exporting country.

10.6 In the event that personal data are transferred directly or indirectly from the UK to a non-EU regulatory authority for the purposes of obtaining and/or maintaining an approval for placing a device on the market or for other regulatory reporting purposes, it may be assumed that such authorities fulfil the need for adequate protection, unless they are specifically excluded by existing UK legislation or by criteria to be established by UK law.

10.7 The procedures for transferring personal data within the same organisation and to and from third parties shall be part of a validated company quality system.

10.8 Any modification or deletion of personal data will be subject to a procedure agreed upon between the Controller in the exporting country and the Controller in the recipient country.

---

7 Since legislation in this area is still evolving, this section of the Code should be regarded as offering guidance only.
11.1 Quality control and quality assurance involving access to and examination of personal data should be performed in accordance with the principles defined in this Code and under applicable local legal and regulatory requirements.

11.2 Source documentation linked to an individual should be maintained at the data source in accordance with applicable procedures governing the storage and retention of personal data and administered under the responsibility of the study investigator or researcher, or otherwise held by a trusted third party.

11.3 Data should be stored according to the archiving legislation and practices in force at each location where data may be held. It should be possible to verify that archiving rules and practices do not impede the execution of quality control or quality assurance activities.

11.4 The same principles for conducting quality control and quality assurance activities should be applied across all research activities falling within the scope of the Code. Further processing of personal data ought to be an acceptable practice within the scope of public health and falls under the framework defined under secondary data processing (cf. Section 7).

11.5 The change or deletion of personal data in databases should be subject to an audit trail. The impact of any modification or deletion should be carefully evaluated by the person or organisation responsible for maintaining the database.

---

8 Within the scope of clinical trial or other studies where personal information may need to be verified to validate the data collected, information in the informed consent process should indicate that quality control (i.e. monitoring) and quality assurance (i.e. auditing) may take place. The written information relating to the informed consent process should include a statement that confidentiality will be maintained by personnel involved in quality control and quality assurance activities.

It is good practice to perform quality control and quality assurance activities as part of data verification. These activities are crucial in order to ensure the validity of recorded data and should be considered to be in the public interest when the data recorded are used for demonstrating efficacy or safety of medical device, or used to make scientific deductions based on population data.
Section 12: Summary of Regulatory Activities involving Personal Data

12.1 Apart from clinical investigations, the medical device industry is under an obligation to carry out certain regulatory activities which involve receipt of personal data. Additionally, certain standard business practices may involve the receipt of personal data. It is not always practicable to obtain informed consent from the individuals concerned. The following notes indicate when such situations may arise. When informed consent cannot be obtained, the industry will use all reasonable efforts to maintain confidentiality of the personal data, and will delete it from its records when operational requirements and regulatory obligations permit.

12.2 The medical device industry frequently needs to provide information and training to support the use of its products. While it is often possible to provide such training without reference to the details of the individuals who receive it, on other occasions a record of participants is required for a Company to demonstrate that it has fulfilled its obligations. In such circumstances, it is often possible to obtain informed consent, but this is not always the case. It would be unreasonable to cancel a training course, or to exclude individuals simply because they have not completed a consent form. In those circumstances, participation in the training should be taken as implied consent.

12.3 There are patients who require medical devices to be tailor made to their requirements - e.g. surgical shoes or artificial limbs. The request for such products comes from a medical practitioner. While a Company would normally request that the practitioner obtain and provide patient consent to personal data being kept on the Company’s files, the Company cannot force the practitioner to do so, and in most cases it would be unethical to approach the patient direct. While it may be possible to anonymise the patient data on the Company's files, inevitably the Company has the key to that data and can identify the patient. Again, it should be assumed that implied consent has been given by virtue of the clinician’s request to the Company.

12.4 The concept of telemedicine (remote operation of medical devices by means of telephone, radio or internet connections) is likely to become a common part of medical treatment. Often Companies are asked to install, maintain or even operate such systems on behalf of a hospital. Again, it is inevitable that the Company will have access to patient data, and while good faith efforts will be made to obtain patient consent, this will not always be possible. Once again, the patient’s agreement with the clinician to participate in such treatment should be treated as implied consent.

12.5 It will be noted that in each of these cases, it is not the desire of the industry to operate without informed consent. However, practical reality is that such consent is not always practicable and that the industry needs to proceed without it.
## DEFINITIONS

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Reference Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous data</td>
<td>Data which are retained in a form in which identification of the data subject is no longer possible.</td>
<td>The Directive</td>
</tr>
<tr>
<td>Clinical Trial</td>
<td>Any investigation in human subjects intended to discover or verify the clinical effects of an investigational product, and/or to identify any adverse reactions to an investigational product(s) with the object of ascertaining its safety and/or efficacy.</td>
<td>ICH GCP ISO 14155</td>
</tr>
<tr>
<td>Code List</td>
<td>A confidential list of all data subjects which links personal identifiers (e.g. name, address, etc) which can directly identify individuals to corresponding research study numbers. Code lists are retained by the treating physician or trusted third party. The identity of the data subject is thus protected and cannot be revealed by sources other than the treating physician or trusted third party.</td>
<td>The Code</td>
</tr>
<tr>
<td>Contractual Partner</td>
<td>Any entity with which a business or legal arrangement exists that involves the exchange or transfer of information or materials involving data subjects. Examples are contract research organisations (CROs), licensing or co-marketing partners, and research institutes or facilities under contract to conduct a study.</td>
<td>The Code</td>
</tr>
<tr>
<td>Controller of the File</td>
<td>The natural or legal persona, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for this nomination may be designated by national or Community law.</td>
<td>The Directive</td>
</tr>
<tr>
<td>Data Privacy Officer</td>
<td>The company official responsible for ensuring the internal application of data protection rules operating procedures in accordance with the Code and the national provisions pursuant to the Directive.</td>
<td>The Code</td>
</tr>
<tr>
<td>Data Processor</td>
<td>A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.</td>
<td>The Directive</td>
</tr>
<tr>
<td>Data Recipient</td>
<td>An individual, company, institution or organisation which receives personal data from a sponsor. This includes regulatory bodies and secondary users such as managed care organisations.</td>
<td>The Directive</td>
</tr>
<tr>
<td>Data Source</td>
<td>An individual, company, institution or organisation which collects or provides personal data. This includes among others, treating physicians, other healthcare professionals, data subjects and laboratories.</td>
<td>The Code</td>
</tr>
<tr>
<td>Encoding</td>
<td>A process whereby true personal identifiers are</td>
<td>The Code</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
<td>Reference Source</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Encryption</td>
<td>A process whereby information is replaced by a cypher (encrypted) in such a way that its true content is only accessible or retrievable to holders of a de-encryption key.</td>
<td>The Code</td>
</tr>
<tr>
<td>Identifiable Person</td>
<td>One who can be identified directly or indirectly, in particular with reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity.</td>
<td>The Directive</td>
</tr>
<tr>
<td>Informed Consent</td>
<td>A process whereby a (data) subject voluntarily confirms their willingness to participate in a research project after having been informed of all aspects of the project that are relevant to the (data) subject's decision to participate.</td>
<td>ICH GCP, ISO 14155</td>
</tr>
<tr>
<td>Ethics Review Committee</td>
<td>An administrative body (also known as an IRB (Institutional Review Board)) established to protect the rights and welfare of human research subjects recruited to participate in research activities conducted under the auspices of an individual or an institution/organisation.</td>
<td>The Code</td>
</tr>
<tr>
<td>Personal Data</td>
<td>Any information relating to an identified or identifiable natural person.</td>
<td>The Directive</td>
</tr>
<tr>
<td>Personal Identifier</td>
<td>Any factor which is specific to the identity of an individual (e.g. name, initials, address, postcode, date of birth, sex, race etc.)</td>
<td>The Code</td>
</tr>
<tr>
<td>Processing</td>
<td>Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.</td>
<td>The Directive</td>
</tr>
<tr>
<td>Quality Assurance</td>
<td>All those planned and systematic actions that are established to ensure that the trials performed and the data are generated, documented (recorded), and reported in compliance with Good Clinical Practice (GCP) and the applicable regulatory requirements(s).</td>
<td>ICH GCP, ISO 14155</td>
</tr>
<tr>
<td>Quality Control</td>
<td>The operational techniques and activities undertaken within the quality assurance system to verify that the requirements for quality of the trial-related activities have been fulfilled.</td>
<td>ICH GCP, ISO 14155</td>
</tr>
<tr>
<td>Recipient</td>
<td>A natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients.</td>
<td>The Directive</td>
</tr>
<tr>
<td>Secondary Data Processing</td>
<td>Activities relating to a research project or to the extension of a research project which aim at analysing individual subject or aggregated data for</td>
<td>The Code</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
<td>Reference Source</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>the purposes of:</td>
<td>a) Making additional observations or drawing additional conclusions beyond those for which the data were originally processed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Extending the use of the data to a new research project.</td>
<td></td>
</tr>
<tr>
<td>Third Party</td>
<td>Any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data.</td>
<td>The Directive</td>
</tr>
<tr>
<td>Trusted Third Party</td>
<td>An individual, company, institution or organisation who is trusted by the controller of the file to view personal data and control access to that data (e.g. via Code Lists).</td>
<td>The Code</td>
</tr>
<tr>
<td>Transborder Data Flow</td>
<td>Transfer of any data, whether or not in an aggregated form, from an EU Member State to a non-EU country, based on the ‘sender-receiver’ principle of identifying a ‘sending source’ in one country and a ‘receiving source’ in the other country.</td>
<td>The Code</td>
</tr>
</tbody>
</table>
REFERENCES


(2) Good Clinical Practice: Consolidated Guideline – ICH Secretariat c/o IFPMA, 30 rue St Jean, PO Box 9, 1211 Geneva 18, Switzerland. May 1997

(3) Council of Europe European Committee on Legal Co-operation (CDCJ). Recommendation no. R(97)5 of the Committee of Ministers of Member States on the protection of medical data. February 1997.