International Pharmaceutical PRIVACY CONSORTIUM

April 6, 2010

International Pharmaceutical Privacy Consortium

WORKING DOCUMENT ON THE COLLECTION, PROCESSING, AND TRANSFER OF BIOMEDICAL RESEARCH AND PHARMACOVIGILANCE DATA

BACKGROUND

The International Pharmaceutical Privacy Consortium (IPPC) is an organization comprised of multinational pharmaceutical companies, all of which conduct business in Europe, North America, and other parts of the world. IPPC member companies sponsor biomedical research with the broad goals of developing and improving drugs and biologics to treat, prevent, and/or better understand a range of diseases and health conditions. The use and transfer of individual-level data is necessary to both drug development and research activities, and to lawfully report to health authorities the adverse events experienced by research participants and patients. These biomedical research and pharmacovigilance activities have long been highly regulated and subject to detailed procedural and ethical requirements, with the central goals of developing new therapies while ensuring the safety of clinical study subjects and patients and empowering individuals to make informed decisions about their participation in research.

The IPPC believes that there is a growing need for a common understanding and a more harmonized approach to protecting the data of individuals in the biomedical research and pharmacovigilance contexts. There have been some differences in interpretation in this area, even though much of the data in question are coded and protected by strict technical and organizational security measures. Patients, clinical study subjects, Data Protection Authorities (DPAs), and pharmaceutical companies would benefit from a widely-accepted and predictable framework for data protection in this sector.

Based on this need for harmonization, IPPC members have developed this Working Document on the collection, processing and transfer of biomedical research and pharmacovigilance data to engage DPAs and other stakeholders in a dialogue on the data protection issues in this sector. This Working Document presents guiding principles and implementation practices that are aspirational in nature. The Working Document has been created as a tool for future progress and does not necessarily reflect the current practices of all IPPC members in all instances. Moreover, in some cases, some companies may have chosen to adopt more stringent protections, and some local interpretations of data protection requirements may require more stringent protections.

This Working Document was developed with data protection requirements of the European Economic Area (EEA) and Switzerland in mind, but individual companies may choose to follow the guiding principles and implementation practices it suggests on a more global basis. The guiding principles and implementation practices are relevant to data collected from patients and clinical study subjects (including healthy volunteers), and also, where specifically noted, address clinical investigators and members of their staff. The IPPC believes that these are appropriate guiding principles and implementation practices, in accordance with applicable data protection laws and requirements, for protecting individual privacy while still enabling the legitimate use and sharing of information to promote and protect public health and advance medical science.

SUMMARY

The IPPC proposes in this Working Document that Key-Coded Data (*see Definitions*, below) used in the context of Biomedical Research should be protected by Data Controllers, and the Data Processors who work on their behalf, using certain rigorous data protection safeguards (such as data security measures), but should not be required to meet all of the standards that apply to directly identifiable Personal Data. This principle addresses the fact that in clinical trials, a mechanism for re-identification of Key-Coded Data by the Clinical Investigator is necessary to meet defined medical, safety and regulatory purposes. In comparison, re-identification by the Pharmaceutical Company Sponsor is excluded in the design of clinical trial protocols and procedures. Pharmaceutical Company Sponsors are by design unaware of the patient's identity, with two limited exceptions which relate to (i) Pharmacovigilance; and (ii) site monitoring.[1] The IPPC recognizes that these narrow exceptions may warrant application of certain data protection requirements, but we urge an application of these requirements in a manner that is proportionate to the risks involved. This approach is consistent with the views of the Article 29 Working Party, which has stated: "[A]lthough data protection rules apply, the risks at stake for the individuals with regard to the processing of [retraceable pseudonymised data] will most often be low, so that the application of these rules will justifiably be more flexible than if information on directly identifiable individuals were processed."[2]

The purpose of this Working Document is to describe potential avenues for pharmaceutical companies and those working on their behalf to meet their responsibilities with respect to Personal Data generally and to identify how principles of data protection are applied to Biomedical Research and Pharmacovigilance activities. The principles that are suggested are respectful of the rights of clinical study subjects and patients, are proportionate to the level of risk involved in sharing Key-Coded Biomedical Research data and Pharmacovigilance data, and are realistic in light of the scientifically-driven data needs of systematic Biomedical Research and Pharmacovigilance activities. The IPPC looks forward to discussing this Working Document further with national DPAs, EU Commission officials and other regulators within and outside of the EEA.

DEFINITIONS

Working definitions are provided below for terms used in this document. These definitions are derived from definitions of similar terms provided in International Conference on Harmonisation (ICH)[3] E6: *Good Clinical Practice* and ICH E15: *Definitions for genomic biomarkers, pharmacogenomics, pharmacogenetics, genomic data and sample coding categories*, as well as

[1] These issues were discussed more thoroughly in the IPPC's comments of February 14, 2008 to the Working Party established under Article 29 of Directive 95/46/EC. The comments addressed the Working Party's Opinion 4/2007 on the Concept of Personal Data.

[2] See p. 18 of Opinion 4/2007 on the Concept of Personal Data.

[3] The International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH) brings together the regulatory authorities of Europe, Japan and the United States and experts from the pharmaceutical industry to discuss scientific and technical aspects of medicinal product registration. As described on the ICH website, "[t]he purpose is to make recommendations on ways to achieve greater harmonisation in the interpretation and application of technical guidelines and requirements for product registration in order to reduce or obviate the need to duplicate the testing carried out during the research and development of new medicines."

from data protection laws, such as the Organisation for Economic Co-Operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the EU Data Protection Directive.

(1) **Anonymised Data:** Initially single or double coded data but where the link between the subjects' identifiers and the unique code(s) is subsequently deleted. In such case, it is no longer possible to trace the data back to individual subjects through the coding key(s).

(2) **Biomedical Research:** The basic research, applied research, or translational research conducted to develop or contribute to knowledge of medicine. For example, Biomedical Research includes research to gain new knowledge about the fundamental processes of life, including how the body works normally. Biomedical Research also includes translation of novel findings obtained from basic research into testable hypotheses for evaluation in clinical trials in human subjects.

(3) **Case Report Form (CRF):** A printed, optical, or electronic document template which is unique for each clinical trial. The CRF is designed to record all of the Study Protocol-required information on each clinical Data Subject. The Clinical Investigator of a study prepares CRFs on each Data Subject and provides the CRFs to the Pharmaceutical Company Sponsor of the study. CRFs are designed to collect only the minimum necessary data and, as such, contain the Data Subject's unique identification code number and various test results or other medical information related to the study, but they do not contain direct personal identifiers such as name, address, or national health number. (The Pharmaceutical Company Sponsor does not need to know the identity of the Data Subject but does need enough information to be able to differentiate among the Data Subjects. For example, it would be difficult to re-identify patient J1R2S3 Age 53, but this information should be sufficient to differentiate him/her from patient A4T5B6 Age 37.)

(4) **Clinical Investigator**: A medical researcher responsible for the conduct of a clinical trial at a trial site.

(5) **Clinical Monitor:** An individual, appointed by a Pharmaceutical Company Sponsor, who is responsible for ensuring that a trial is conducted and documented properly. A Clinical Monitor's duties include checking the accuracy and completeness of the CRF entries, source data/documents, and other trial-related records against each other.

(6) **Data Controller:** The legal person or entity that alone or jointly with others determines the purposes and means of the processing of Personal Data.

(7) **Data Processor:** The legal person or entity that processes Personal Data on behalf of the Data Controller. Data Processors may process Personal Data only in accordance with the instructions of the Data Controller. Data Processors are contractually required to provide a level of data protection safeguards equivalent to those required of Data Controllers.

(8) **Data Subject:** An identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, by a person with reasonable access to the data. For purposes of this Working Document, Data Subject includes an individual in his or her capacity as a participant in biomedical research, a patient, and a person reporting pharmacovigilance information.

(9) **Key-Coded Data:** Key-Coded Data have information that identifies a particular Data

Subject replaced with a subject identification code (that is not derived from information related to the Data Subject), such that taking into account all the means reasonably likely to be used, it is possible only to trace the data back to the particular Data Subject by referencing the key (*i.e.*, a listing of the Data Subjects' names and their associated subject identification codes). In the Biomedical Research context, Key-Coded Data are associated with a unique code number and do not carry such direct personal identifiers as name, address, or national health number. Generically speaking, the terms "coded data", "key-coded data" and "pseudonymised data" are often used interchangeably. Coding of data is the usual mechanism used within the research community for protecting a Data Subject's privacy. Coding restricts identification of Data Subjects' personal information to specific individuals involved in the research project, such as Clinical Investigators, while still allowing for the addition of further research information as the study proceeds, clinical monitoring and research oversight. The ability to de-code data and re-identify Data Subjects permits auditing by drug regulatory authorities in order for them to verify the source and quality of safety and efficacy data collected during clinical trials and subsequently used in an application for a license to market a medicine.

(10) **Personal Data:** Personal Data means any information relating to a Data Subject.

(11) **Pharmaceutical Company Sponsor:** A pharmaceutical company that takes responsibility for the initiation, management, and/or financing of a clinical trial.

(12) **Pharmacovigilance:** The science and activities relating to the detection, assessment, understanding and prevention of adverse events or any other drug-related adverse effects.

(13) **Processing:** Any operation or set of operations that is performed upon Personal Data, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, alignment or combination, blocking, redaction, erasure or destruction.

(14) **Study Protocol:** A document that describes the objective(s), design, methodology, statistical considerations, and organization of a trial.

IPPC Guiding Principles and Implementation Practices

The following guiding principles are based on the fundamental principles enshrined in the OECD Guidelines and incorporated into the EU Data Protection Directive and national implementing laws. The "Implementation Notes" below seek to apply these principles for Personal Data in a proportionate manner to Biomedical Research and Pharmacovigilance activities.

(1) **Fair and Lawful Processing:** Personal Data should only be processed for purposes that are fair and lawful.

Implementation Notes for Biomedical Research and Pharmacovigilance:

a. The processing of data for purposes of Biomedical Research or Pharmacovigilance should be considered fair and lawful if conducted in accordance with this Working Document and with local and international health regulatory requirements and regulations for the conduct of Biomedical Research / Pharmacovigilance.

(2) **Data Collection:** Personal Data should only be processed for specified and legitimate purposes.

Implementation Notes for Biomedical Research and Pharmacovigilance:

a. A specified and legitimate purpose should be considered: (i) one which provides the Data Subject with sufficient information to make a reasonably informed decision as to whether to provide his or her data; or (ii) one that has been approved by a Research Ethics Committee (REC) overseeing Biomedical Research, or (iii) one that is necessary for protecting public health, including activities related to Pharmacovigilance.

(3) **Minimum Necessary Data:** The processing of Personal Data should be limited to those data that are necessary for the intended purposes.

Implementation Notes for Biomedical Research and Pharmacovigilance:

a. The ICH E2D guideline on *Post-Approval Safety Data Management: Definitions and Standards for Expedited Reporting* states that "Patient and reporter identifiability is important to avoid case duplication, detect fraud, and facilitate follow-up of appropriate cases. The term identifiable in this context refers to the verification of the existence of a patient and a reporter." The guideline recommends the inclusion of the following patient details in expedited reports: initials; other relevant identifiers (patient number, for example); gender; age, age category (e.g., adolescent, adult, elderly), or date of birth; concomitant conditions; medical history; and relevant family history. Capture of these data elements is important for accurate Pharmacovigilance reporting purposes. Companies that comply with this ICH E2D guideline and collect recommended data elements should be deemed in compliance with the "Minimum Necessary" principle.

(4) **Accuracy and Completeness:** Personal Data should be factually accurate and, as far as possible, up-to-date. Reasonable and appropriate measures should be implemented to correct, amend or delete inaccurate or incomplete Personal Data.

Implementation Notes for Biomedical Research and Pharmacovigilance:

a. Pharmaceutical Company Sponsors of clinical studies are responsible for ensuring that such studies are conducted, recorded, and reported in accordance with the Study Protocol, standard operating procedures (SOPs), Good Clinical Practice (GCP), and applicable regulatory requirements. One of the purposes of trial monitoring is to ensure that reported trial data are accurate, complete, and verifiable from source documents.

(5) **Data Retention:** Personal Data should ordinarily be kept for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Personal Data may be kept for longer periods for scientific use, subject to appropriate safeguards (e.g., strict limits on physical and electronic access).

Implementation Notes for Biomedical Research and Pharmacovigilance:

a. Data should be retained in compliance with relevant laws and regulations that govern retention and archiving of data by pharmaceutical companies. Data may be retained for as long as necessary to support the submission and maintenance of marketing authorizations around the world. Data also may be maintained in a

form which permits only restricted access for purposes such as conducting future Biomedical Research, analyzing adverse events, and responding to regulatory requests.

b. *Legal Proceedings:* Personal Data may be retained for longer periods where such Personal Data are relevant to pending legal proceedings such as civil litigation or a government investigation. Any retention of Personal Data for legal proceedings should be conducted in accordance with the applicable laws and regulations of the territories in which the Personal Data are collected and subsequently processed.

(6) **Consent:** Informed and freely given consent for the processing of Personal Data should be obtained from the Data Subject (or his/her legal representative) prior to any data processing unless (i) the Data Subject is deceased, or (ii) obtaining consent is impractical and either (a) processing does not cause physical or emotional harm to the Data Subject, and/or (b) there is an overriding public health interest such as Pharmacovigilance.

Implementation Notes for Biomedical Research and Pharmacovigilance:

a. Drug safety reporting and Pharmacovigilance are critical public health activities. Privacy rights of Data Subjects can be protected without impeding these activities. Health care providers that contact drug manufacturers to report adverse events may provide notice of the disclosure to the affected Data Subject. However, reporting of adverse events to pharmaceutical sponsors and to drug regulatory agencies should not be contingent upon consent. Obtaining consent is not always possible in the context of the voluntary reporting of spontaneous adverse drug experiences and the monitoring and surveillance of safety data. Accordingly, the important public health interest in conducting these activities in a timely and effective manner should constitute sufficient grounds for the processing of data for these purposes provided that the processing (i) does not support measures or decisions with respect to any particular Data Subject, and (ii) does not otherwise cause physical or emotional harm to the Data Subject or any other person. Such data should, however, be safeguarded with adequate technical and organizational controls.

b. To the extent practicable, Pharmaceutical Company Sponsors should anticipate future uses of Key-Coded Data at the time of its collection from Data Subjects. Such future uses should be indicated in the notices/consents provided to the individual Data Subject. For example, sponsors' informed consent forms should set forth, in specific terms where known or otherwise in general terms, if additional analysis of data may be performed at a later time in order to support further development of the drug or future drugs and/or support disease understanding, or because of requests from health authorities to provide further data on patients who have taken the drug. However, it is recognized that it is not always feasible to anticipate all specific future uses at the time of data collection.

c. Where a future use of Key-Coded Data was not anticipated at the time of initial consent, it may not be possible or appropriate to re-identify Data Subjects in order to obtain consent to conduct secondary Biomedical Research. For example, several years after an initial research project, the original research physician and participants may no longer be associated with a given hospital and may not be able to be located. Obtaining consent to use data for secondary

Biomedical Research purposes may also involve a disproportionate delay and level of resources.

Secondary data analysis plays an important role in research and development of life-saving treatments. Secondary Biomedical Research using Key-Coded Data should be permissible by pharmaceutical company researchers who do not have access to the key and are therefore not able to identify Data Subjects without expending disproportionate resources. A precondition for such use would be the implementation of appropriate technical and organizational controls to prevent the data from being misused or disseminated more broadly than necessary for the research activity. Pharmaceutical company researchers should also consider the sufficiency of anonymised data for their research purposes.

d. In certain cases, an initial Key-Coded Data set may not meet a researcher's needs. For example, in epidemiological, health outcomes or longitudinal Biomedical Research, it may be of great scientific value for a researcher to be able to supplement a data set received from one source (or time point) with data sets from other sources and to combine data that relates to the same patient. This would enable a more robust analysis of risk factors, outcomes, and extended follow-up time. To do this, an external third party would link identifiable records received from different sources as relating to the same individual and then pseudonymise the data. However, pharmaceutical company researchers would continue to receive only Key-Coded Data and not have access to direct patient identifiers or the key code.

The REC with jurisdictional oversight over the relevant Data Subjects or medical information should be consulted prior to conducting a Biomedical Research project that involves the processing of directly identifiable Personal Data. The REC would decide if the affected individuals need to be contacted to obtain consent (or reconsent). A newly provided specific consent may not be necessary if a prior, more general consent is deemed satisfactory to permit secondary research, or if the REC grants a waiver of consent. In granting a waiver, an REC should consider the necessity of the Personal Data for the research purposes, the potential harms and benefits of the research, the practicality of obtaining consent, and the expectations of individuals. When Personal Data are used for Biomedical Research purposes pursuant to these procedures, direct identifiers should be avoided or concealed to the extent practicable.

e. *Withdrawal of consent:* The Data Subject has the right to withdraw consent to participate in further Biomedical Research at any point, in which case no additional data should be collected from him or her. A Data Subject may withdraw consent without adverse consequences to the quality of any clinical care that may be given to him or her. When consent is sought, the Data Subject should be informed of the procedure for withdrawal and its implications. Therefore, the consent should cover what happens with collected data in the case of the Data Subject's withdrawal. The consent should inform Data Subjects that it may not be possible to identify and remove already-collected data from a research project in such circumstances and that data already collected may need to continue to be used to preserve scientific validity, in compliance with health regulatory and data protection requirements.

(7) **Access and Amendment by Data Subject:** The Data Subject has the right to request information about the types or categories of Personal Data that are being

processed about himself or herself. A Data Subject's access to Personal Data about himself or herself may be temporarily suspended where necessary to preserve the integrity of an ongoing clinical study. The Data Subject also has the right to request correction or deletion of Personal Data shown to be incorrect.

Implementation Notes for Biomedical Research and Pharmacovigilance:

a. With respect to access during prospective, blinded clinical studies, treatment allocations should not be revealed unless deemed essential to ensure the safety or the well-being of the Data Subject, because to unblind the study may unduly infringe the rights of other participants by compromising the integrity of the study.

b. Data subjects should only have the right to correction, amendment or deletion of *inaccurate* or *incomplete* Personal Data. The modification or removal of data that are believed to be accurate and complete may compromise research data integrity.

c. Access to Key-Coded Data cannot be provided without reference to the key. Data Subject requests for access to Key-Coded Data should be directed towards the holder of the key. For example, access to Personal Data generated in clinical studies should be facilitated by the Clinical Investigator, who is responsible for maintaining the key codes and any associated identifiable medical records. It is the Clinical Investigator's responsibility to inform a Pharmaceutical Company Sponsor of any data reported in a CRF that later is determined to be inaccurate or incomplete.

(8) **Confidentiality:** Except to the extent required for proper performance of their duties, Pharmaceutical Company Sponsor personnel whose responsibilities require them to have direct access to Personal Data should take all reasonable precautions to keep confidential such Personal Data received by them or disclosed to them in the course of their work.

Implementation Notes for Biomedical Research and Pharmacovigilance:

a. Employment contracts and contractor agreements should include appropriate stipulations that require compliance with all applicable laws, including data privacy laws.

b. Access to Personal Data obtained for Pharmacovigilance purposes should be restricted to those conducting or providing support to Pharmacovigilance activities.

c. Personal Data of clinical study subjects observed during Clinical Monitor or Pharmaceutical Company Sponsor oversight visits to study sites should not be taken off-site, disclosed to third-parties, or shared with other individuals within or outside of the company for purposes not related to such oversight activities.

d. Personal Data of site personnel may be taken off-site by a Clinical Monitor or a Pharmaceutical Company Sponsor in the following circumstances, provided it is protected according to contractual and legal requirements:

i. To document the roles and responsibilities of site personnel.

ii. For the purposes of reporting deviations and/or deficiencies identified at a site visit.

(9) **Data Security:** Reasonable and appropriate technical, organizational, and physical

controls should be used to protect Personal Data from loss or destruction, or unauthorized access, use, or disclosure in violation of these guiding principles and implementation practices.

Implementation Notes for Biomedical Research and Pharmacovigilance:

a. Pharmaceutical Company Sponsors of clinical studies should make Clinical Investigators aware of their responsibility to maintain key codes in a secure location that can be accessed only by approved and authorized personnel under appropriate safeguards.

b. Examples of good practices that companies may wish to consider in developing security policies and procedures include the following:

- Assigned security responsibilities.
- Processes for conducting ongoing security risk assessments.
- Security plans for each major system and network.
- Log-in monitoring procedures.
- Contingency plans, including business continuity and disaster recovery plans.
- Requirements for integration of security throughout system life cycles.
- Data backup processes.
- Security auditing processes.
- Documentation of all system and network configurations.
- Employee awareness and training.
- Oversight of third-party Data Processors.
- Control of access to information that resides on data storage devices.
- Password usage requirements.
- Control of access to information that can be displayed, printed, and/or downloaded to external storage devices.
- Monitoring and tracking the receipt and removal of electronic media containing personal data from a facility.
- Media disposal and re-use.
- Integrity checks.
- Safeguards over the transmission and storage of data.
- Firewall security.
- Anti-malware safeguards.
- Processes for implementing security software updates and patches.
- Physical access controls of data center rooms and buildings.
- Security incident response procedure.

(10) **Cross-Border Transfers:** Companies may transfer Personal Data collected in the EEA and Switzerland to third parties outside of the EEA and Switzerland only if adequate protections are in place to safeguard the rights of Data Subjects. A transfer should also be deemed appropriate if one of the following conditions is met:

i. The Data Subject has consented to the transfer.

ii. The transfer is necessary or legally required on important public health grounds.

iii. The transfer is necessary for the performance of a contract between the Data Subject and the Data Controller.

Implementation Notes for Biomedical Research and Pharmacovigilance:

a. The transfer of data collected in the EEA and Switzerland to drug regulatory authorities, company affiliates, contractors, and partners outside of the EEA and Switzerland should be permitted without consent for purposes of Pharmacovigilance reporting, including services and technologies that facilitate Pharmacovigilance reporting.

b. Companies that transfer Personal Data collected in the EEA and Switzerland to affiliates, contractors, and partners outside of the EEA and Switzerland should require that recipients process the Personal Data in accordance with these guiding principles and implementation practices.

c. Consent should be an adequate basis for cross-border transfers of Personal Data on Clinical Investigators and other clinical study staff.

(11) **Responsibility of Data Controller:** The Data Controller should be responsible for addressing compliance with these guiding principles and implementation practices, and local requirements in each relevant country. The Data Controller also should be responsible for defining the contractual obligations of the Data Processor. Therefore, the processing of Personal Data should be carried out only upon instructions of the Data Controller or its designee, including its parent company, where applicable.

Implementation Notes for Biomedical Research and Pharmacovigilance:

a. Data Controllers should require Data Processors to comply with the Controller's data protection policies and procedures or comparable standards consistent with these guiding principles and implementation practices.

b. *Policies and Procedures:* The Data Controller should develop appropriate governance frameworks (e.g., policies, procedures, and other quality measures) to address compliance with these guiding principles and implementation practices.

c. *Training:* Company personnel involved in collecting, handling, and otherwise processing Personal Data should receive training on the Data Controller's data protection policies and procedures. Outside vendors should meet the requirements of the Data Controller's data protection policies and procedures or their own policies and procedures if consistent with these guiding principles and implementation practices.