December 23, 2009

INTERNATIONAL PHARMACEUTICAL PRIVACY CONSORTIUM

COMMENTS IN RESPONSE TO THE CONSULTATION ON THE LEGAL FRAMEWORK FOR THE FUNDAMENTAL RIGHT TO PROTECTION OF PERSONAL DATA

I. INTRODUCTION

The International Pharmaceutical Privacy Consortium (IPPC) is an organization formed in 2002 and comprised of chief privacy officers and other data protection professionals from research-based, global pharmaceutical companies, all of which conduct business in the European Union. Membership and mission of the IPPC is described in Attachment A.

The European Commission's "Consultation on the legal framework for the fundamental right to protection of personal data" provides a welcome opportunity to assess the effectiveness of the Data Protection Directive (EU Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data) in achieving a balance that protects individual privacy while still enabling the use and sharing of information to protect public health and advance medical science. With this in mind, it is appropriate to examine not only the letter of the Directive but how it has been implemented in the EU member states. Although the Directive was intended to promote harmonisation of information handling practices across the EU, divergent interpretations of the Directive have resulted in sometimes significant disparities in its implementation.

Pharmaceutical companies process and share information for biomedical research and pharmacovigilance using highly controlled processes that are grounded in respect for individual rights, patient safety, and compliance with strict clinical research laws, regulations and guidelines such as the International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use Guidelines for Good Clinical Practice ("ICH GCP")[1] and the European Clinical Trials Directive.[2] Maintaining data confidentiality and subject privacy are essential to these activities. Privacy-protecting safeguards have been incorporated throughout the extensive regulatory systems under which pharmaceutical companies must operate and have been integrated into standard processes for data collection and use. Data protection authorities and patients alike must have confidence that medical research and pharmacovigilance data are collected and processed in a way that respects the fundamental rights of data subjects. It is equally important to understand the way data are used during medical research and pharmacovigilance activities and to appreciate the real-world implications of greatly restricting or prohibiting certain data flows that are vital to life-saving research and safety reporting activities.

II. COMMENTS

A. International Data Flows

The Data Protection Directive poses a challenge for multinational companies who need to share information among affiliates and with vendors and regulators across international borders.

[1] CPMP/ICH/135/95ICH.
[2] Directive 2001/20/EC. Further elaboration of principles of GCP is outlined in the Good Clinical Practice Directive (2005/28/EC).

Pharmaceutical companies need to transfer data outside of the European Economic Area for a variety of purposes. These include the transfer of:

- pharmacovigilance data to foreign health authorities, as required by applicable national regulations;
- data concerning research subjects for purposes of analysis and submission of applications to drug regulatory authorities for marketing authorisation (product license);
- information on clinical investigators conducting research sponsored by the company, for required reporting purposes.

Multinational pharmaceutical companies also may transfer data outside of the European Economic Area for other business purposes such as:

- consolidated storage of data collected in multiple countries in a single database hosted on a company server located in a country outside of the EEA;
- coordinated processing of data twenty-four hours per day by utilizing regional data processing centers located in different time zones outside of the EEA; and
- centralized analysis of data collected in multiple countries by a global team based in a country outside of the EEA.

Mechanisms exist to enable the transfer of data to countries outside of the EEA that have not received an adequacy determination; however, each of these mechanisms has disadvantages or limitations, and none comprehensively fulfils all of a multinational company's international data transfer needs. For example:

- The Safe Harbour negotiated with the United States applies only to transfers to the US.
- The Model Clauses are administratively burdensome in that they require a web of rigid, individual contracts. Sometimes hundreds of contracts are required to cover transfers between all affiliates of an organization. Keeping contracts up-to-date and reflective of changing corporate structure can be a difficult undertaking.
- Binding Corporate Rules have not historically been able to be used absent a lengthy and burdensome approval process, and they can only be used for intra-organizational transfers. Moreover, while important improvements have been made to streamline the BCR approval process through a cooperation procedure, there remains the problem that in some member states national law does not allow for the concept of unilateral declarations, which effectively makes approval of a BCR in these countries impossible.

In addition, some EU member states have layered a requirement to obtain prior authorization from the data protection authority on top of the requirement to either use one of the above mechanisms or transfer the data pursuant to one of the derogations for which cross-border transfers are permitted. Such layering of requirements causes undue delays that are incompatible with meeting business needs and foreign regulatory reporting deadlines.

The IPPC suggests several alternative approaches for addressing some of the limitations of existing cross-border transfer mechanisms. These include (i) modelling a new compliance option on the EU-US Safe Harbour 'Onward Transfer' mechanism; (ii) incorporating Binding Corporate Rules as a

compliance option into the Directive itself, to ensure acceptance of this concept in all member states; and (iii) recognizing the adoption of voluntary industry codes as a means to ensure an adequate level of data protection in the destination country.

i. Safe Harbour Onward Transfer Mechanism

The EU-US Safe Harbour 'Onward Transfer' mechanism provides a potential model for another compliance option for transferring data globally. The Onward Transfer Principle provides as follows:

> To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles.[3]

Pursuant to this Principle, onward transfers from a Safe Harbour member company in the US to another data controller can take place if the data subject has been given notice of the transfer and has had the opportunity to opt out. Moreover, onward transfers to a data processor are permitted without overly prescriptive contractual language being required.[4] Instead, the requirement is for only a written agreement requiring the processor to provide at least the same level of privacy protection as that required by the Safe Harbour Principles. The Onward Transfer Principle thereby ensures that personal data are protected when transferred globally without being unduly restrictive.

The IPPC recommends that a compliance option modelled on the Onward Transfer Principle be added to the list of explicit derogations in Article 26 of the Data Protection Directive.[5] Specifically, transfers to a data controller should be permitted if the data subject has been given notice of the transfer and has the opportunity to opt out. Transfers to a data processor should be permitted where a written agreement requires such third party to provide the same level of privacy protection as the data controller.

[3] Safe Harbor principles, available at: http://www.export.gov/safeharbor/eg_main_018247.asp.

[4] The endnote to the Onward Transfer Principle states that ''It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures.''

[5] Moreover, even before such derogations are added to the Directive, Article 26(2) gives individual data protection authorities the flexibility necessary to permit global transfers that are conducted in accordance with the Onward Transfer Principle. Article 26(2) provides that a transfer or set of transfers of personal data to a third country which does not ensure an adequate level of protection can be authorized where the data controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of data subjects.

IPPC RECOMMENDATION #1

Simpler legal processes should be established to enable international transfers of personal data. Cross-border data transfers to third party data controllers should be permitted where notice and an opt-out option have been provided to the data subject. In addition, transfers to a third party that is acting as an agent should be permitted where a written agreement requires such third party to provide the same level of privacy protection as the data controller.

ii. Improvements to BCR Mechanism

As noted, in some member states national law does not allow for the concept of unilateral declarations. Since a BCR is essentially a unilateral declaration by a corporate entity that members of the corporate group will adopt certain privacy protections, the failure to recognize the legal effect of a unilateral declaration means that BCRs cannot be approved in such member states. The IPPC therefore recommends the incorporation of Binding Corporate Rules as a compliance option into Article 26 of the Data Protection Directive itself, to ensure acceptance of this concept in all member states.

Once a data controller has received approval of its BCR, the IPPC also recommends that international data transfers to third party service providers be permitted where the provider is legally bound (e.g., via the service agreement) to adhere to the data controller's BCR. This would simplify the paperwork necessary to achieve compliance with data protection laws.

IPPC RECOMMENDATION #2

Important improvements have been made to streamline the BCR approval process through a cooperation procedure, but certain member states still do not recognize the validity of BCRs for transferring data. European law should explicitly recognize BCRs as a valid transfer option. Moreover, in line with Recommendation #1, above, transfers to a third party that is acting as an agent should be permitted where a written agreement requires such third party to adhere to the data controller's BCR.

iii. Voluntary Industry Codes

Finally, another possible option that would reduce burdens for both organizations and data protection authorities would be to recognize the adoption of voluntary industry codes as a means to ensure an adequate level of data protection. For example, in the pharmaceutical industry, a voluntary code could address the use and transfer of coded (pseudonymised) research data (discussed more fully in Section B, below). Article 27 of the Directive allows industry codes to be approved by member state DPAs and/or the Article 29 Working Party. However, some data protection authorities are of the view that voluntary industry codes cannot be used as a means for compliance with international data transfer requirements. The IPPC notes that the legal underpinning for a DPA's recognition of a voluntary industry code as providing an adequate level of data protection would not differ from that underpinning BCR approval (i.e., recognition that a unilateral declaration by an organization creates a legal obligation). Nevertheless, recognizing that some member states do not recognize the legal effect of unilateral declarations, the IPPC recommends that Articles 26 and 27 of the Directive be amended to enable voluntary industry codes to be used as a mechanism for transferring data globally.

IPPC RECOMMENDATION #3

EU law should authorize the Commission to approve voluntary industry codes as a mechanism for transferring data internationally.

iv. Request for Prior Authorization

Where notification for prior checking purposes is required before an international transfer can be conducted, this further delays a data controller's processing activities. For example, despite the fact that the model clauses have been approved by the European Commission, some countries nevertheless require an exporting data controller to seek prior authorization before using them. Such time consuming requirements serve little purpose and ultimately undermine the goal of the free movement of data. Prior authorization should be required only where none of the derogations of Art. 26(1) applies and the transfer will not be conducted pursuant to one of the approved transfer mechanisms.

IPPC RECOMMENDATION #4

Prior authorization to internationally transfer personal data should be required only in exceptional circumstances. Where a transfer is pursuant to an already approved mechanism (e.g., consent of the data subject, the model clauses for cross-border transfers, etc.), prior authorization should not be required.

B. Pseudonymised (Coded) Data

A pragmatic balance is needed to both protect individual privacy and also facilitate data access for bona fide public health and medical research purposes. Indeed, this is the objective of Articles 8(4), 11(2), and 12(2) of the Directive, which authorize member states to exempt certain data privacy requirements when processing is conducted for purposes of scientific research under globally recognised frameworks such as ICH GCP and the European Clinical Trials Directive. The need for a pragmatic balance is particularly relevant in the context of pseudonymised data such as key-coded biomedical research data. It is impractical and an impediment to research to apply the full 'bundle of protections' specified in the Data Protection Directive to key-coded data that are highly unlikely ever to be re-identified. Therefore, for example, international transfers of key-coded data should not be restricted when the recipient located in another country does not have access to the key. The IPPC also proposes that pharmaceutical researchers should not be required to obtain a subject's specific consent before using key-coded data for secondary research when the key necessary to identify data subjects is held by a third party under an obligation of confidentiality. Under such circumstances, general consent for secondary research should be sufficient (*e.g.*, consent to analyze the study data for general biomedical research purposes such as understanding disease mechanisms).

The Article 29 Working Party appeared to recognize this point when it stated in its paper on the concept of 'personal data' that "[A]lthough data protection rules apply, the risks at stake for 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." The IPPC fully agrees with this comment and urges that this principle be incorporated into the Directive itself, to ensure its application in a harmonised manner at the member state level.

The ability of researchers to have access to key-coded data collected in prior clinical or other research studies and to analyze such data for "secondary" research purposes is important to the development of new medicines. These secondary purposes could, for example, involve further examination of the disease or condition in question, or examination of some unanticipated, secondary benefit or risk of an investigational drug. Secondary research purposes have not been, nor usually can they be, specifically determined at the time the primary research is undertaken. Therefore, they can only be described in broad strokes or general terms in the initial informed consent process. Data subjects should be permitted to consent to having their data used for unspecified medical research, so long as their consent is freely given.

Researchers working for a sponsor to conduct secondary research analyses have no need, intent or reasonably available means to identify patients. Indeed, the purposes of secondary research typically are similar to retrospective epidemiological analyses and include, among other things, further analyses of factors involved in disease and treatment of disease. In both primary and secondary research using key-coded data, researchers within the sponsor organisation do not have access to the confidential key that would reveal data subjects' identities. Therefore, the risk of harm to data subjects arising from such secondary research analyses is de minimus at most.

IPPC RECOMMENDATION #5

Risks associated with the processing of re-traceable pseudonymised data are low. Data protection requirements applicable to pseudonymised data should therefore be correspondingly flexible. For example, pharmaceutical researchers should not be required to obtain a subject's specific consent before using key-coded data for secondary research when the key necessary to identify data subjects is held by a third party under an obligation of confidentiality. Similarly, international transfers of key-coded data should not be restricted when the recipient in another country does not have access to the key. The principle that data protection requirements applicable to pseudonymised data should be correspondingly flexible to the risks associated with the processing of such data should be explicitly incorporated into European law.

C. Data Controller / Data Processor Distinction

The distinction between whether a party is a "data controller" or a "data processor" has important practical consequences in terms of data protection compliance responsibilities. In spite of this, the distinction between who is a data controller and who is a data processor often does not adequately describe the relationship between the relevant parties, and there is often a lack of clarity as to whether a particular party is a "data processor" or a "data controller." For example, when a service provider makes any decision regarding the most appropriate way to provide its services, such as what technology to use in processing personal data, some legal commentators argue that it no longer acts upon the data controller's instructions and should be considered a data controller itself. Other legal observers have argued that such choices are inherent in the activity of any data processor and do not in

and of themselves trigger data controller responsibilities. Indeed, the controller / processor distinction can be so vague that in certain instances member state data protection authorities have taken different views on whether a party is acting as a controller versus a processor.

In the pharmaceutical industry, this issue frequently arises in the context of an agreement between a research sponsor and a contract research organization (CRO) to oversee a clinical study. While a pharmaceutical sponsor could be viewed as determining the purposes for which personal data are collected and used in a study, day-to-day oversight of a study may be the responsibility of the CRO, and the CRO may have considerable latitude in determining the best means of providing its services. This can lead to uncertainty as to the appropriate categorization of each party for purposes of the Data Protection Directive.

The IPPC urges the Commission to consider whether the data controller / data processor distinction continues to provide a useful means of distinguishing the roles of the parties involved in a particular activity given the rate of technological change and new business models which are being adopted by companies in order to remain competitive. A great deal of time and effort is spent trying to determine the appropriate categorization of the parties involved in a data processing activity, and it is reasonable to question whether this time might be better spent actually ensuring that appropriate data privacy and security safeguards are in place. This is not intended to minimize the importance of designating one party with a European presence or appointed European representative to be accountable for data processing activities, but it would be beneficial to rethink or at least further clarify the data controller / data processor distinction.

IPPC RECOMMENDATION #6

The controller / processor distinction creates confusion without substantively increasing data subject protections. The parties involved in a relationship that involves data processing governed by the Directive should be permitted to designate which party will be legally accountable for data processing activities as long as the designated party has a European presence or has appointed a European representative.

D. Data Controller Registration

The European Commission and Article 29 Working Party have previously looked at the issue of notification of data processing activities to data supervisory authorities and concluded that much can be done to simplify and harmonise the processes across member states.[6] Nevertheless, implementation disparities and widespread confusion about notification requirements remain, and in some member states, notification could be greatly streamlined.

The IPPC also encourages each DPA to carefully consider the purpose of its registration scheme and to only collect the minimum necessary data to accomplish this purpose. If the purpose is simply to place the DPA on notice that an organization is processing personal data so that the DPA can more efficiently exercise its enforcement powers (e.g., through written inquiry or on-site inspection), then

[6] See, e.g., Article 29 Working Party "Report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union" (WP 106).

certain minimal categories of information may be needed for these purposes. On the other hand, if the purpose, in fact, is to provide meaningful notice to the public at large of an organization's data processing activities, then more detailed information may be needed. In this latter case, notification provided to data protection authorities ought to be deemed to largely fulfil an entity's obligation to provide notice of its data processing activities to data subjects.

IPPC RECOMMENDATION #7

Requirements to notify data supervisory authorities of data processing activities should be simplified and harmonised across member states. Data protection authorities should carefully consider the purpose of their registration schemes and only collect the minimum necessary data to accomplish these purposes.

E. Accessibility of Information

Harmonization of data protection laws and guidelines across EU member states would greatly simplify compliance for multinational companies. Short of such harmonization, however, there are steps that the Commission could take to facilitate compliance. In particular, Article 29 Working Party documents and all member state guidance / policy documents on a particular subject should be made available on a single web site. While the Justice and Home Affairs Data Protection web site makes some attempt to do this, it is incomplete. For example, whistle blowing guidance is available only for Spain and Belgium, even though many other countries have issued guidance on this topic. A "one stop resource center" maintained by the Commission would be of great practical value and is a simple way to help organizations understand their compliance obligations.

IPPC RECOMMENDATION #8

Further efforts should be made to ensure the easy accessibility of EU member state data protection laws and guidelines. The availability of all member state guidance and policy documents on a single web site would ease compliance burdens.

F. Process for Public Consultation

The Data Protection Directive establishes at a high-level general rules on the lawfulness of the processing of personal data. In applying the Directive to specific circumstances, however, much is left to the interpretation of data protection authorities. The IPPC recommends the establishment of uniform standards for the conduct of taking decisions on the interpretation of the Directive and national implementing laws. Such transparency and opportunity for stakeholder involvement should extend to the advisory opinions issued by the Art. 29 Data Protection Working Party given the importance of these opinions to interpretation of European data protection law. Effective public participation in the taking of decisions enables the public to express, and the decision-maker to take account of, opinions and concerns which may be relevant to those decisions. This increases the accountability and transparency of the decision-making process and contributes to public awareness.

IPPC RECOMMENDATION #9

Uniform procedures should be established to enable meaningful stakeholder involvement in the taking of decisions on the interpretation of the Directive and national implementing laws.

III. CONCLUSION

The IPPC is grateful for this opportunity to provide comments in response to the Commission's Consultation, and we welcome further dialogue on these critical issues.

APPENDIX A: INTERNATIONAL PHARMACEUTICAL PRIVACY CONSORTIUM

MEMBERS

The IPPC is an association of companies that face worldwide responsibility for the protection of personal health information and other types of personal data. Members of the IPPC include:

- Abbott Laboratories
- AstraZeneca
- Bristol-Myers Squibb
- Elan Pharmaceuticals, Inc.
- Eli Lilly and Company
- GlaxoSmithKline
- Merck & Co., Inc. *(operating as Merck Sharp &*
- Novartis
- Pfizer Inc.
- Roche
- sanofi-aventis
- Takeda Pharmaceuticals

MISSION

The IPPC works to promote responsible privacy and data protection practices by the research-based, global pharmaceutical industry. Maintaining data confidentiality and subject privacy are essential to clinical research, pharmacovigilance, and other activities of the pharmaceutical industry. The IPPC seeks to increase awareness of privacy and data protection issues and to engage government in a dialogue about the need for data to support cutting edge biomedical research and other public health activities. The IPPC pursues opportunities to collaborate with government and other stakeholders to develop data protection practices that enhance data subject privacy.

GOALS

The IPPC goals are to:

- Engage government and stakeholders in the biomedical research and healthcare communities in a constructive dialogue on significant issues of privacy and data protection.
- Serve as a resource for sound analyses of privacy and data protection requirements and compliance tools tailored to the pharmaceutical industry.
- Serve as a forum for industry dialogue and promote responsible privacy and data protection practices.
- Promote consistent privacy and data protection standards that can be achieved on a worldwide basis.
- Remain on the leading edge of privacy and data protection.

SCOPE OF ACTIVITIES

The IPPC advances understanding of existing and emerging data protection and security rules in Europe, the US, and other key countries. The Consortium engages regulators and policymakers in the following areas:

- Biomedical research
- Pharmacovigilance
- Sales and marketing
- Market research
- Human resources programs
- Other corporate programs

International Pharmaceutical
PRIVACY CONSORTIUM

1500 K Street NW • Suite 1100 • Washington DC 20005 USA
Telephone +1 202 230 5142 • Facsimile +1 202 842 8465 • Website www.pharmaprivacy.org