14 January 2011

INTERNATIONAL PHARMACEUTICAL PRIVACY CONSORTIUM

COMMENTS IN RESPONSE TO THE CONSULTATION ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION

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 Appendix A.

The IPPC welcomes this opportunity to provide comments on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions entitled "A comprehensive approach on personal data protection in the European Union" (hereinafter "the Communication"). The IPPC supports the aims of the Commission to sustain a high level of data protection and to provide legal certainty and clarity for stakeholders. These comments supplement our submission of December 2009 in response to the "Consultation on the legal framework for the fundamental right to protection of personal data"[1] and of July 2010 in response to the "Future of Data Protection" Background Paper circulated to stakeholders.[2] For convenience, we have included a summary of the recommendations we made in those submissions in Appendix B. We also have been provided the opportunity to review the comments of the Association of Clinical Research Organizations (ACRO) on the Communication, and we wish to express our full support of those comments.

II. COMMENTS

A. Key-Coded Data for Biomedical Research Purposes

The Communication states: "[T]here are numerous cases where it is not always clear, when implementing the Directive, . . . whether individuals enjoy data protection rights and whether data controllers should comply with the obligations imposed by the Directive."[3] The Communication cites key-coded data as an example of a case where further measures may need to be specified at the European level in order to ensure coherent application of data protection rules. The IPPC agrees that further clarification of data protection measures applicable to key-coded data is necessary; however, we believe that the concept of "key-coded" data in the biomedical research field has a well-established meaning and corresponding set of protections provided by other legal and regulatory frameworks applicable to data processing in this field. Accordingly, we request that when considering further clarification, the Commission distinguish "key-coded" data in the context of biomedical research from other types of data coding that may not be complemented by comparable controls.

---

[1] *Copy available at:* http://www.pharmaprivacy.org/download/IPPC%20Comments%20to%20European%20Commission%20on%20Data%20Privacy%20Consultation.pdf. Hereinafter "IPPC December 2009 Submission."

[2] *Copy available at:* http://www.pharmaprivacy.org/download/Joint%20IPPC-ACRO%20Submission%20to%20European%20Commission%20Future%20of%20Data%20Protection%20Consultation.pdf. Hereinafter "IPPC July 2010 Submission."

[3] § 2.1.1.

We wish to highlight the special nature of and protections already applied to key-coded data in biomedical research. The IPPC has previously commented upon the need for a pragmatic balance to both protect individual privacy and also facilitate data access for bona fide public health and medical research purposes. This has included calling for the EU data protection legal framework to distinguish requirements applicable to key-coded data for biomedical research purposes from requirements applicable to more directly identifiable personal data.[4]

In clinical research, coding of data is used by clinical investigators to report study data to the research sponsor. The investigator maintains the key at the study site, and representatives of the sponsor are permitted access to the key only for purposes of clinical monitoring and auditing. The clinical investigator is otherwise prohibited by principles of good clinical practice (GCP) and professional confidentiality from revealing research subject identities to the sponsor. While field monitors working on behalf of the sponsor may have access to identified patient information at the study site, such individuals are bound by confidentiality obligations and prohibited from removing this identified personal information from the study site or sharing it more broadly with other sponsor employees or representatives. Researchers working for or on behalf of a sponsor to conduct scientific analyses using the key-coded data have no need, intent or reasonably available means to identify specific research subjects.

It is impractical to apply the full protections specified in the Data Protection Directive to key-coded biomedical research data that are highly unlikely ever to be re-identified. The legal frameworks governing biomedical research, such as ICH GCP and the European Clinical Trials Directive, already provide ample protections for such data. Protections that are applied under the Data Protection Directive should be proportionate to the risks involved. Protections that are appropriate to key-coded biomedical research data are summarized below, as are suggested modifications to the Data Protection Directive, where necessary. (For a full discussion of the protections that we believe should apply to key-coded biomedical research data, please see the *IPPC Working Document on the Collection, Processing, and Transfer of Biomedical Research and Pharmacovigilance Data.*[5])

- Clinical investigators, the holders of the key, are responsible for obtaining informed consent from data subjects.
- Data subjects' rights of access and amendment, as well requests to withdraw consent should be directed toward the holder of the key rather than the holder of the key-coded data.
- International transfers of key-coded data for biomedical research purposes should not be restricted when the recipient located in another country does not have access to the key and contractual or legal restrictions prohibit re-identification of the data subjects.[6]
- General consent for secondary biomedical research using key-coded data should be sufficient to permit such processing (e.g., consent to analyze the study data for general biomedical research purposes such as understanding disease mechanisms).

---

[4] *See* IPPC July 2010 Submission; IPPC December 2009 Submission, *supra* note 1, at pp. 5-6; IPPC Comments to the Article 29 Working Party Concerning Opinion 4/2007 on the Concept of Personal Data, *available at* http://www.pharmaprivacy.org/download/IPPC%20Comments%20on%20Art%2029%20WP%20Opinion%20on%20Personal%20Data.pdf.

[5] *Available at* http://www.pharmaprivacy.org/download/Working%20Document%20on%20Data%20Project%20in%20Biomedical%20Research%20and%20PV.pdf.

[6] This approach is consistent with FAQ 14 of the Safe Harbor Framework for the transfer of personal data to the United States.

- Coding should be recognized as a measure for ensuring that privacy is embedded into the design of biomedical research studies and as a security measure that significantly reduces risks to data subjects in the event of a breach. Breach notification requirements should not apply to key-coded data, unless the key is breached together with the data.
- Registration of data processing activities by sponsors should not be required with respect to processing of key-coded data for biomedical research purposes.
- The "Right to be Forgotten" must be carefully construed and applied in the context of biomedical research. For example, once a data subject agrees to participate in a biomedical research study, the scientific integrity of the study analyses depends upon the ability to accurately track and correlate data about that data subject up until the point that the data subject either completes participation in the study or until the data subject withdraws from the study, whichever is sooner. Upon withdrawal, no further data about the data subject is collected; however, it is essential that the data about that study subject that already has been collected be retained for the duration of time in which all other data for the particular biomedical research study or studies are retained.

"Data Minimisation"

The Communication states that the Commission will examine ways of strengthening the principle of data minimisation.[7] The IPPC supports the principle of collection and use of the minimum personal data reasonably necessary to accomplish the intended purpose of the processing. While the phrase "data minimisation" may be useful as a shorthand way of saying this – i.e., processing the minimum personal data reasonably necessary to accomplish the intended purpose of the processing – the Commission should make absolutely clear what it means by the use of this phrase. We believe that collection of personal or key-coded health data reasonably related to the endpoint of a particular biomedical research study (i) to assess specific or adjunct health conditions, (ii) to assess or compare the effectiveness of a particular course of treatment or treatments, or (iii) to evaluate related health outcomes is essential to advancing healthcare innovation and to reducing the overall cost of healthcare to society. Accordingly, we recommend that in the context of data processing in the biomedical research and health care fields, data controllers should be granted latitude to determine what data is reasonably necessary to accomplish their purposes.

A related point concerns the inclination of some data protection authorities to question the perspectives of the relevant experts in a field as to what data elements are, in fact, "necessary." In some contexts (e.g., sales and marketing) it may be appropriate for data protection authorities to question claims as to what data elements are reasonably needed; in other areas, however, this judgment often lies beyond the expertise of data protection officials, and the consequences can be enormous. For example, in the context of drug adverse event reporting, significant public health stakes should warrant that data protection authorities defer to the experience and wisdom of health authorities and relevant experts in the field. In contexts such as this where public health is impacted and the stakes are high, data protection authorities who disagree with the intended scope of data processing should be obligated to show that personal data processing is unreasonably excessive or not reasonably related to the intended purposes of processing.

[7] § 2.1.3.

Privacy Information Notices

The IPPC takes note of the Commission's intention to consider drawing up one or more privacy information notices to be used by data controllers.[8] In principle, the IPPC agrees that information notices should be as clear as possible and plain language used, and we would appreciate any example information notices the Commission is able to provide to facilitate this end. Nevertheless, because we believe that privacy information notices must necessarily be tailored to the specific data processing activities in question, we caution against mandating overly detailed language that is not industry, field or purpose specific.

Breach Notification

The Communication indicates that the Commission will examine the modalities for the introduction of a general personal data breach notification requirement. The IPPC recommends that notification requirements be triggered only where a breach poses a substantial risk of harm to data subjects. Requiring notification in other circumstances will divert resources from other, more tangible privacy and security safeguards. In particular, as noted earlier, we do not believe that notification obligations should apply to breaches of key-coded biomedical research data unless the key is also accessed or acquired by unauthorized persons.

Data Subject Access Requests

The Communication states that the Commission will examine ways of improving the modalities for the exercise of the right of access to personal data about oneself. Examples listed include the introduction of deadlines for responding to data subject access requests and providing that access should be ensured free of charge as a principle.[9] The IPPC urges the Commission to consider the administrative burdens and associated costs to data controllers as one factor in its examination of how to improve the implementation of the right of access. In the case of decentralized systems and databases, deadlines shorter than 30 calendar days following the receipt of a request in most cases will be infeasible for many data controllers.

It must also be noted that the exercise of the right of subject access presents unique issues in the context of biomedical research. First, as noted above, subject requests for access to data generated in a clinical study should be directed towards the relevant clinical investigator rather than the pharmaceutical sponsor. This is because the pharmaceutical sponsor maintains only key-coded data and has no readily available means to re-identify the data. Second, the right of access should not be deemed to extend to exploratory biomedical research test results that have not been analytically validated and/or whose clinical meaning is unknown. In exploratory biomedical research, researchers may perform a multitude of tests and analyses in an attempt to identify correlations between biomarkers[10] and a variety of biological states. These tests and analyses may be conducted in basic or early

[8] § 2.1.2.
[9] § 2.1.3.
[10] A "biomarker" is a biological indicator of a process, event, or indicator.

translational[11] research laboratories under conditions that do not have rigorous quality control and chain of custody mechanisms in place to assure the analytical validity of the results for patients. Providing research subjects with access to non-validated test or exploratory research results may be misleading, result in unnecessary follow up testing or premature treatment decisions, and cause confusion, anxiety and/or emotional distress.[12] Moreover, as noted above, such exploratory biomedical research is conducted using key-coded or pseudonymised data. Researchers conducting exploratory biomedical research often have no direct interaction with patients, and may be multiple steps removed from the initial biological sample and clinical data collection. A better alternative to individual data subject access to exploratory biomedical research study results is for researchers to publish scientifically valid global results of such exploratory research in recognized peer-reviewed scientific and medical journals.

Genetic Data

The Communication states that the Commission will consider explicitly mentioning genetic data as a sensitive category of data.[13] The IPPC requests that the Commission clarify specifically what type of information it is considering including under the term "genetic data." For example, is the term intended to only refer to information about an individual's genetic tests, or would it also include information about the genetic tests of family members or even the manifestation of a disease or disorder in a family member? Is the term intended to refer only to information about the presence or absence of a gene or chromosome, or a variant thereof, that has been scientifically demonstrated to be associated with significant risk of a disease, disorder, condition or syndrome? Is the term intended to include information related to the 99.99 percent of genome sequences that are common to all humans, or would it only include information related to genetic variations?

The IPPC questions the purpose of singling out genetic data as a special category of data (i.e., "genetic exceptionalism"). Indeed, an independent Expert Group convened by the European Commission's Directorate-General for Research has concluded that "genetic exceptionalism is both scientifically unjustified and not helpful in addressing ethical and societal issues."[14] To the extent specific genetic data is predictive of a disease, disorder or syndrome, such data already is included within the scope of sensitive health information. To the extent genetic data has not been determined to provide any actual predictive value, it is unclear why such data should necessarily be treated as sensitive.

---

[11] "Translational research" refers to the branch of medical research that attempts to more directly connect basic research to patient care. In drug development, it refers to the conversion of basic research advances into products that can be tested on humans.

[12] L.G. Dressler and E.T. Juengst, *Thresholds and Boundaries in the Disclosure of Individual Genetic Research Results*, 6 AM. J. BIOETHICS 18, (2006); F.M. Facio, *One Size Does Not Fit All*, 6 AM. J. BIOETHICS 40, 41 (2006); Ravitsky and Wilfond, *Disclosing Individual Genetic Results to Research Participants*, 6 AM J. BIOETHICS 8, 10 (2006).

[13] § 2.1.6.

[14] INDEPENDENT EXPERT GROUP, EUROPEAN COMMISSION'S DIRECTORATE-GENERAL FOR RESEARCH, ETHICAL, LEGAL AND SOCIAL ASPECTS OF GENETIC TESTING: RESEARCH, DEVELOPMENT AND CLINICAL APPLICATIONS (2004), at 33, *available at* http://ec.europa.eu/research/conferences/2004/genetic/pdf/report_en.pdf. *See also* COUNCIL FOR INTERNATIONAL ORGANIZATIONS OF MEDICAL SCIENCES (CIOMS), PHARMACOGENETICS: TOWARDS IMPROVING TREATMENT WITH MEDICINES (2005); European Federation of Pharmaceutical Industries and Associations (EFPIA) "Key Messages Surrounding Pharmacogenetics" at § 3.1, *available at* http://www.efpia.eu/content/default.asp?PageID=559&DocID=1365.

Codes of Conduct

The IPPC supports a flexible European data protection framework with strong incentives to encourage accountable self-regulation by those who process personal data. Therefore, we are encouraged by the statement in the Communication that the Commission will examine means of further encouraging self-regulatory initiatives, include the active promotion of Codes of Conduct. The IPPC is aware of the approval to-date of only one EU-wide code of conduct, which we believe suggests that greater incentives are needed to promote the adoption of such codes. The advantage of an industry code of conduct would be far clearer if such codes could be used as a means for compliance with international data transfer requirements, including data processing involving multiple stakeholders and collaborators within or supporting a particular industry. The IPPC recommends that Articles 26 and 27 of the Directive be amended to enable voluntary industry codes containing appropriate accountability mechanisms to be used as a mechanism for transferring data globally.

Harmonisation of Laws and Clarification of Legal Framework

The IPPC strongly supports the Commission's commitment in the Communication to examine the means to achieve further harmonisation of data protection laws at the EU level. The lack of harmonisation of national data protection laws creates great administrative burden. Harmonisation is needed not only of national data protection laws, but also of national data protection laws with other laws, such as health regulatory requirements. For example, data protection laws should be made consistent with pharmacovigilance reporting guidelines and requirements.

As IPPC Member Companies have operations and/or conduct business in almost all EU countries, as well as in other countries outside of the EU, we strongly support clarification around the legal framework for controllers, processors and representatives in the territory where controllers or processors are based outside of the EU. For example, the existing legal framework often leads to multiple affiliates of the same group of companies entering into redundant agreements with the same data processor based outside of the EU and to multiple interpretations from country to country as to whether a particular form of non-sensitive personal data processing requires consent or registration.

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
- Baxter International
- Bristol-Myers Squibb
- Elan Pharmaceuticals, Inc.
- Eli Lilly and Company
- GlaxoSmithKline
- Merck & Co., Inc. *(operating as Merck Sharp & Dohme in most countries outside USA)*
- 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.
- Provide leadership on privacy and data protection issues.

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

APPENDIX B: IPPC DECEMBER 2009 RECOMMENDATIONS

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.

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.

IPPC RECOMMENDATION #3

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

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.

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.

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.

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.

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.

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.