INTERNATIONAL PHARMACEUTICAL PRIVACY CONSORTIUM

COMMENTS IN RESPONSE TO THE CALL FOR EVIDENCE ON EU DATA PROTECTION PROPOSALS

I. INTRODUCTION

The International Pharmaceutical Privacy Consortium (IPPC) is an organization formed in 2002 and comprised of chief privacy officers and other privacy professionals from a number of research-based global pharmaceutical companies, all of which conduct business in the United Kingdom and other parts of the European Union. Membership and mission of the IPPC is described in Attachment A. We appreciate this opportunity to provide feedback on the European Commission's proposed General Data Protection Regulation.

The IPPC takes note of the Commission's stated goals in proposing to reform the Data Protection Directive. These are (i) to modernize the EU legal system for the protection of personal data in order to meet challenges resulting from globalization and the use of new technologies; (ii) to strengthen individuals' rights while at the same time reducing administrative formalities so as to ensure a free flow of personal data within the EU and beyond; and (iii) to achieve a consistent and effective application of data privacy requirements throughout the EU. The IPPC supports these goals, and we will refer back to them in our comments on the proposed Regulation.

II. PHARMACEUTICAL INDUSTRY USES OF PERSONAL DATA

Two of the primary uses of personal data within the pharmaceutical industry are for (A) biomedical research and (B) pharmacovigilance.

A. Biomedical Research

Over the last century, medical science has transformed human health and dramatically increased life expectancy. The life-saving treatments available today were made possible by an environment that fostered medical research. The scientific process used in medical research relies on the ability to effectively collect, analyze and re-analyze patient health information. Pharmaceutical companies collect patient health information created in controlled research settings (e.g., clinical trials to investigate an experimental drug), as well as real-world patient health data.

B. Pharmacovigilance

Pharmacovigilance is the science of activities relating to the detection, assessment, understanding and prevention of drug adverse effects or any other drug-related problem. Adverse events include a range of negative or unexpected reactions to a drug – from relatively minor irritations to potentially life threatening conditions. Internationally recognized Good Pharmacovigilance Practices are followed in the collection, analysis, and reporting of patient health information related to adverse events.

III. IPPC VIEWS ON THE PROPOSED REGULATION

The IPPC has participated in the development by the European Federation of Pharmaceutical Industries and Associations (EFPIA) of a Position Paper concerning the proposed Data Protection Regulation. This Position Paper is provided in Attachment B. The Position Paper represents our principal views on the proposed Regulation. We will use this opportunity to elaborate upon the positions outlined in that paper. Section III.8, below, also addresses some additional issues.

1. The Proposed Regulation Recognizes the Importance of Scientific Research, Although Certain Technical Clarifications Are Needed.

Article 83 of the Proposed Regulation allows the processing of personal data for scientific research purposes if (i) the research purposes cannot be achieved through the use of anonymised data, and (ii) the personal data have been pseudonymised, to the extent feasible. Article 83 implicitly recognizes the public interest in advances in medical science, and it places appropriate conditions around the use of personal data for scientific research purposes in order to protect individual privacy.

Medical research today already takes place under highly controlled conditions. Health regulations are designed to not only ensure scientific integrity, but to protect the rights and interests of patients and research subjects. In the European Union, the *Clinical Trials Directive 2001/20 of 4 April 2001 on the implementation of good clinical practice in the conduct of clinical trials* provides the relevant framework. This framework, which in fact reflects internationally agreed norms for the conduct of medical research, requires the review of research protocols by independent ethics committees, the informed consent of individuals prior to their participation, and the disguising of patient identities to protect patient privacy. Only "key-coded data" (or data which have had information that identifies a particular data subject – i.e., name, address, national health number, etc. – replaced with a subject identification code that is not derived from information related to the data subject) is reported to pharmaceutical companies sponsoring research studies, not directly identifiable data.

Under the Data Protection Directive, pharmaceutical companies have been informed by data protection authorities in some member states that they must delete key-coded data once it is no longer necessary for the primary study. This hinders pharmaceutical researchers' access to and use of patient information vital to biomedical research and innovation. In contrast, under the Proposed Regulation, Article 17(3) and Article 83 allow personal data to be retained for scientific research purposes. The IPPC believes that the Proposed Regulation's approach to processing of personal data for scientific research purposes represents an improvement over the Directive, and we support these provisions in the proposal.

The IPPC does recommend several technical clarifications of the proposal to ensure the proper application of Article 83:

a. Article 6 Should Be Revised To Clarify that Processing in Accordance with Article 83 Is a Separate and Sufficient Basis for Processing of Personal Data. Article 6(2) states that "Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83." Read alone, Paragraph 2 is

clear that the processing of personal data in accordance with Article 83 is lawful. However, a degree of ambiguity is created by the language of Paragraph 1, which states that "Processing of personal data shall be lawful only if and to the extent that at least one of the following applies . . ." The IPPC therefore suggests that Paragraph 2 be made a subparagraph of Paragraph 1 or the "only if" language of Paragraph 1 be deleted.

b. Scientific Research Conducted in Accordance with Article 83 Should Be Added to Article 6(4) as a Legal Basis to Further Process Personal Data. Article 6(4) indicates that the further processing of personal data should be allowed only where such processing is compatible with those purposes for which the data have been initially collected. The public interest in scientific advancement warrants adding scientific research to those uses of personal data for which further processing is permitted (or clarifying that scientific research is already included among such permitted uses), provided such processing is conducted in accordance with the data protections of Article 83. This addition (or clarification) is consistent with the purpose of Article 83.

2. The Proposed Regulation Recognizes the Importance of Pharmacovigilance.

Article 81(1) of the Proposed Regulation permits the processing of personal data for public health purposes, such as ensuring high standards of quality and safety of medicinal products. This recognition of the public interest in pharmacovigilance is an improvement over the existing Directive.

As noted above, Good Pharmacovigilance Practices are followed in the collection, analysis, and communication of safety information to patients, healthcare practitioners, consumers, and regulators. Nevertheless, under the Directive, some data protection authorities have questioned the need to collect certain patient information for pharmacovigilance purposes, often arguing that the collection of certain data elements is more than "minimally necessary" for safety reporting purposes. The Proposed Regulation represents an improvement over the Directive by explicitly stating that the processing of personal data necessary for ensuring high standards of quality and safety of medicinal products is permissible. The proposal could be improved still further by explicitly recognizing that health authorities are in the best position to decide what data are necessary for pharmacovigilance purposes.

3. A Regulation is the Appropriate Legislative Vehicle for Achieving EU Harmonisation.

The IPPC supports the Commission's efforts to further harmonise data protection requirements in the EU through a regulation. The inconsistent application of privacy requirements impedes global clinical trials and creates challenges for the collection and reporting of safety data concerning medicines. As it stands currently, IPPC members must keep track of 27 different data protection laws and associated interpretations. These divergences make compliance difficult and costly. For example, regulators disagree on whether the collection of patient initials and full dates of birth in clinical trials and for pharmacovigilance purposes complies with "data minimisation" principles. They also disagree on whether "key-coded data" constitutes "personal data" subject to data protection requirements. They sometimes disagree on whether a particular research entity, like a contract research organisation, is classified as a controller or a processor. They even sometimes disagree on whose law applies to a particular data processing activity.

Prior efforts to harmonise interpretations of the Data Protection Directive through opinions of the Article 29 Working Party have fallen short. First, given its workload, the Article 29 Working Party has been unable to address sector-specific concerns regarding divergences in interpretation and application of the Directive. Second, even where the Working Party has issued opinions, those opinions have not been binding upon member state data protection authorities.

Because a regulation would be directly binding within all EU member states without requiring transposition into national law, and because under the proposal a single point of authority (i.e., the Commission) would have responsibility for issuing most interpretive guidance, the IPPC believes that a regulation offers the best hope of achieving "a consistent and effective application of data privacy requirements throughout the EU".

4. Certain Data Protection Requirements Should Not Apply to Key-Coded Research Data.

As noted, in compliance with the Clinical Trials Directive and international standards for clinical investigations, patient identities are disguised before clinical trial data are reported by study sites to pharmaceutical companies. Researchers at pharmaceutical companies use key-coded data to conduct analyses, and to develop, test, and confirm research hypotheses. The keys are held solely at study sites by clinical investigators (healthcare professionals) who are prohibited under obligations of good clinical practice in place since the Nuremberg Code of 1947, as well as obligations of professional confidentiality, from revealing research subject identities except during field audits or where necessary to protect the health of a particular research subject.[1] Researchers at pharmaceutical companies have no reason to identify the data subjects behind the key-coded data as this is not necessary for their research activities.

With respect to this key-coded data:

a. Transfer to a Third Country Should be Permitted (Art. 42): Key-coding should be added as a recognized means for appropriately safeguarding personal data prior to transferring it to a recipient located in a third country. A transfer of key-coded data for scientific research purposes, while the key stays within the EU, should not require any further regulatory authorisation.

Today, clinical trials are typically conducted using multiple sites around the world. The key-coded data reported by each of these sites is put into a centralised database and made available to researchers around the world working on the research project. (As noted, the keys themselves never

[1] Pharmaceutical companies are required under health regulations to employ field monitors to verify that patient data reported by clinical investigators is accurate. Such monitoring and auditing is designed to prevent fraud and ensure the validity of the study. While field monitors working on behalf of a pharmaceutical sponsor may have access to directly identifiable patient information at the study site for this purpose, they are bound by confidentiality obligations and prohibited from removing this directly identifiable personal information from the study site or sharing it more broadly with other sponsor employees or representatives.

Research subject identities may also need to be revealed so that serious adverse events can be addressed as quickly as possible. Such events are rare and occur only where there is a need for direct, immediate communication between a clinical investigator and the safety team at a pharmaceutical research sponsor.

leave the sites.) The research workforce is global. This reflects the reality that the experts on particular aspects of a study often reside in different countries. Nevertheless, none of these researchers using the key-coded data has any need, intent or reasonably available means to identify specific study subjects, except as strictly necessary for safety reasons.

Under the Data Protection Directive, in many member states, the transfer of key-coded data outside the EU to global research databases is forbidden absent prior authorization of the data protection authority. Seeking such approval is often a *pro forma* exercise, yet it can consume weeks or months of time, resulting in delays in researchers' ability to analyse the data. The new Regulation should recognize that research is a global endeavour necessitating global data transfers, and key-coded data is appropriately protected.

b. Breach Notification to Supervisory Authority Should Not Be Required (Art. 31): Key-coded data should not be subject to the Regulation's mandated breach notification requirements that apply to data that directly identifies a natural person, provided the key is not compromised. Key-coded data is not readily identifiable, and, therefore, a breach poses virtually no privacy risks.

A requirement to notify supervisory authorities of all situations leading to a loss of personal data or to the possibility of unauthorised access to personal data regardless of whether there is a material risk of harm will result in over-notification. Supervisory authorities would be inundated by such notifications, resulting in reduced overall effectiveness. Where personal data is already protected through encryption, key-coding, or other mechanisms, a breach notification requirement risks becoming another "administrative formality". It would be far more effective to only require notification to supervisory authorities of breaches where there is a material risk of harm.

5. Clarifications Are Needed as to the Requirement to Conduct Data Protection Impact Assessments.

The IPPC believes that certain clarifications are needed in Article 33 with respect to data protection impact assessments. Most importantly, it should be clarified that a single data protection impact assessment is permitted to cover uses of personal data that are of a similar nature and present the same privacy risks. A requirement to conduct multiple, duplicative assessments for similar data processing activities would add burden and costs without substantively increasing data protection.

A new privacy impact assessment should be required only where a process or project poses substantially new or different privacy risks from what has been analyzed in the past. Where a similar process or project has undergone a privacy impact analysis in the past, only those aspects of the process or project that are new or different should be required to be analyzed anew. For example, the collection, analysis, and reporting of information concerning adverse events that patients have experienced while taking a medication presents common privacy risks irrespective of the specific medication or geography concerned. A single privacy impact assessment should be sufficient to identify the privacy risks involved in pharmacovigilance activities and appropriate risk mitigation steps. Similarly, the use of key-coded data for scientific research purposes usually poses the same privacy risks even in different clinical studies. Only those aspects of a clinical study that present different privacy risks – for example, the use of a new clinical research organization or a new electronic data capture system –

should require re-analysis. Secondary research using key-coded data also usually presents common privacy risks, and the same logic should apply to determining the extent of any privacy impact assessment that is needed.

6. The Proposed Definition of "Genetic Data" Is Overly Broad.

The proposed definition of "genetic data" in Article 4(10) is overly broad. The breadth of the current definition would turn inherited characteristics such as eye and hair colour into sensitive categories of data requiring heightened protections. A more targeted definition based on existing international standards would be to define "genetic data" as follows: "Information on the hereditary characteristics, or alteration thereof, of an identified or identifiable person, obtained through nucleic acid analysis."

7. The Procedure for Adoption of Delegated Acts Must Be Inclusive of Stakeholders.

Throughout the Proposed Regulation, the Commission is authorized to adopt "delegated acts" to provide further guidance and details on the operation of the regulation. *(See Art. 86; see also, e.g., Arts. 14(7), 17(9), 81(3), and 83(3).)* The IPPC appreciates that this authority will enable the Commission to issue sector-specific guidance while at the same time providing a means for the Regulation to be adaptable over time.

Recital 129 states with respect to such delegated acts that "It is of particular importance that the Commission carry out appropriate consultation during its preparatory work, including at expert level." The IPPC fully agrees with this statement. In particular, we would encourage consultation with researchers on the application of Article 83(3) concerning limitations on the rights of notice and access where necessary for scientific research purposes, as well as on the application Article 17(3) concerning the retention of personal data necessary for public health or scientific research purposes.

8. Other Comments.

While the above comments represent the IPPC's priority concerns, we also wish to note our views concerning the following points:

- The drawing up of codes of conduct on the application of the regulation to specific sectors would seem to be a sensible approach for ensuring that the specific features of the various data processing sectors are taken into account. Therefore, we support this proposal in Article 38.
- We recognize the importance of the concepts of data protection by design and by default, and we support the inclusion of these principles in the regulation (Art. 23).
- Special attention is appropriate to the issue of data protection and minors. We note that in the research context, stringent safeguards governing the approval and conduct of paediatric studies have been established. These measures are designed to assure that minors in clinical trials are protected from exploitation and that their rights and safety are of paramount concern in any clinical investigation.

- Penalties applied to infringements of the regulation should be commensurate to the resulting harm to data subjects as opposed to penalizing organisations for administrative errors. In all cases, whether to impose a penalty should be discretionary, as should be the minimum level of any penalties. Penalties should take into account an organisation's good faith efforts to comply with the Regulation.
- Further clarity should be provided on the application of the regulation to entities headquartered outside of the EU. In particular, clarity would be helpful around how to determine the applicable EU member state supervisory authority for an entity located outside the EU.
- Further consideration should be given as to how to enable international data transfers while at the same time ensuring that personal data is appropriately protected. The IPPC is encouraged by work underway to examine how the principle of accountability could be applied to cross-border data transfers to accomplish this.
- A 24-hour timeframe for notifying supervisory authorities of personal data breaches is too short for compiling the information required to be reported. We recognize that the language of Article 31(1) requires providing notification within 24-hours only "where feasible", but the creation of a baseline standard that is too short will result in rushed, inaccurate reporting.
- The maximum level of administrative fines allowed under Article 79 should be based on the revenues of the responsible data controller or processor. It should not include revenues of other companies that may be related as a "group of undertakings", but which had no responsibility for the data processing activity in question.
- The IPPC understands the reference in Recital 26 (concerning the definition of personal data relating to health) to "a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes" as referring to a health plan beneficiary number or a national identification number used to track a patient in the health care system. This is how the same language is used in ISO 27799. For the avoidance of confusion, we would encourage the addition of the following at the end of the above phrase: ". . . , except for a number, symbol, or particular assigned to an individual for purposes of Article 83(b)." A number, symbol, or particular assigned to an individual for purposes of Article 83(b) is an identifier, but it is not intrinsically data *relating to health* (unless combined with health data).

The IPPC appreciates this opportunity to provide feedback on the Proposed Regulation. Please feel free to contact us with any questions on this submission or our positions more generally.

ATTACHMENT 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
- Amgen Inc.
- Astellas Pharma, Inc.
- AstraZeneca Pharmaceuticals
- Baxter International, Inc.
- Bristol-Myers Squibb
- Eli Lilly and Company
- GlaxoSmithKline
- Merck & Co., Inc. *(operating as Merck Sharp & Dohme in most countries outside USA)*
- Novartis
- Pfizer Inc.
- Roche/Genentech
- Sanofi
- Shire
- 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

ATTACHMENT B

EFPIA POSITION STATEMENT ON REFORM OF THE EU DATA PROTECTION DIRECTIVE

EFPIA welcomes the Commission's efforts to further harmonise data protection requirements in the EU through a regulation. The inconsistent application of privacy requirements impedes our industry's ability to conduct meaningful biomedical research that leads to the discovery of new medicines, and it creates particular challenges for the collection and reporting of safety data concerning medicines.

EFPIA also welcomes recognition that the public interest in advances in medical science warrants **special rules on the collection and use of personal data for medical research purposes** *(Art. 83)*, and **justifies collection and use of data for public health purposes** *(Art. 81(1))*. Both of these activities already take place under highly controlled and regulated conditions which are designed to protect patient privacy.

However, **EFPIA believes that there are still some changes needed to avoid unintended impacts on medical research**:

- **Application of certain requirements to key-coded data:** patient identities are disguised before clinical trial data are reported by study sites to pharmaceutical companies. Unless an individual takes extraordinary measures, "key-coded data" can be re-identified only through access to a key held securely by each study site.
  - **Key-coding should be added as a recognized means for appropriately safeguarding personal data prior to transferring it to a third country** *(Art. 42).* A transfer of key-coded data for scientific research purposes should not require any further authorisation or consultation.
  - **Key-coded data should not be subject to the Regulation's mandated breach notification requirements that apply to data that directly identifies a natural person, provided the key is not compromised** *(Art. 31).* Key-coded data is not readily identifiable, and, therefore, a breach poses virtually no privacy risks.
  - **Scientific research conducted in accordance with Art. 83 should be added to Art. 6(4) as a legal and compatible basis to further process personal data**.

- **A single data protection impact assessment should be permitted to cover processing of personal data that is of a similar nature and presents the same privacy risks** (Art. 33). A requirement to conduct multiple, duplicative assessments for similar data processing activities would add administrative burden without substantively increasing data protection.
  - A single assessment should be sufficient to identify potential risks and risk mitigation strategies related to similar uses of key-coded data for scientific research purposes. The same applies to the collection and reporting of information on drug adverse events.

- The **proposed definition of "genetic data" is overly broad** and would turn inherited characteristics such as eye and hair colour into sensitive data requiring heightened protections *(Art. 4(10)).*

- A **more targeted definition based on existing international standards** would be: "Information on the hereditary characteristics, or alteration thereof, of an identified or identifiable person, obtained through nucleic acid analysis."

- **The process for adoption of delegated acts by the Commission should require consultation with relevant stakeholders** *(Art. 86 and others)*.
  - For example, researchers should be consulted on the application of Art. 17(3) (retention of personal data necessary for public health or scientific research purposes) and Art. 83(3) (limitations on the rights of notice and access where necessary for scientific research purposes).