
**Joint Submission of the International Pharmaceutical Privacy Consortium
and Association of Clinical Research Organizations in Response to the
Stakeholders' Consultations "Future of Data Protection" Background Paper**

Introduction

The International Pharmaceutical Privacy Consortium (IPPC) is an organization comprised of chief privacy officers and other data protection professionals from research-based, global pharmaceutical companies. Similarly, the Association of Clinical Research Organizations (ACRO) represents the world's leading clinical research organizations (CROs) that provide a wide range of specialized services across the entire spectrum of drug development to research sponsors. Member companies of both organizations conduct significant business and employ thousands of professionals in the European Union. As the drug development process is a shared enterprise, IPPC and ACRO have common cause regarding the regulatory framework that governs the transfer, processing and retention of clinical trial and pharmacovigilance data.

In response to the 1st July 2010 stakeholders consultation on the review of the data protection legal framework, IPPC and ACRO have come together in support of one key proposal for consideration that we feel addresses numerous issues affecting both the clinical research process and pharmacovigilance. Whereas our activities centre on drug development, scientific and medical advancement, and ultimately human health, collectively we are committed to assisting the Commission with enhancing the data protection framework in order to support the vital continuance of research and pharmacovigilance in the European Union. Further, our perspective comes from long-standing success with the protection of highly sensitive personal data in this regard. It is with these ideas in mind that we put forward the following comments.

Key-Coded (Pseudonymised) Data for Scientific Purposes

Questions 17 and 19 of the Stakeholders Consultations Background Paper ask whether the existing legal framework should be clarified in regards to the processing of personal data related to health and with respect to provisions in the Data Protection Directive addressing "data for scientific purposes". The IPPC and ACRO believe that the existing data protection legal framework should distinguish requirements applicable to key-coded data for scientific purposes from requirements applicable to more directly identifiable personal data.

The European Clinical Trials Directive 2001/20 of 4 April 2001 on the implementation of good clinical practice and the conduct of clinical trials lays down a legal framework focusing on a process of disguising identities by using key-coded data. Key-coded data are data that have had information that identifies a particular data subject (e.g., name, address, national health number) 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).¹ Coding by its very nature, therefore, is a strong technical measure that protects data subject privacy, and key-coded data should be recognized as an intermediary category of data, between fully identifiable personal data and anonymised data.²

In the scientific context, it is important to distinguish the concepts of data individuation (i.e., the differentiation of data as being related to separate individuals) from data subject identification (i.e., discovery of the "identity" of the data subject). Scientists often have the need to differentiate data as being related to separate individuals, in order to perform accurate statistical analyses, without having any need or desire to actually identify the subjects of the data. In clinical research, for example, 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.

A pragmatic balance is needed both to protect individual privacy and also to 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

¹ The terms "coded data", "key-coded data", and "pseudonymised data" are often used interchangeably. The IPPC and ACRO would be happy to work with the Commission to develop a common taxonomy. The definition of "key-coded data" we have provided here is similar to the definition of "single coded data" provided in International Conference on Harmonisation E15 (Definitions for genomic biomarkers, pharmacogenomics, pharmacogenetics, genomic data and sample coding categories).

² Austrian law, for example, already treats "indirectly personal data" as a distinct category of data.

Clinical Trials Directive. The need for a sensible balance is particularly relevant in the context of pseudonymised data such as key-coded biomedical research data. It is impractical and an impediment to biomedical research 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. In particular:

- Data subjects' rights of access and amendment 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 scientific 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.
- 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).
- Coding should be recognized as a technical security measure that eliminates risks to data subjects in the event of a breach (which otherwise would necessitate breach notification).
- Registration of data processing activities should not be required with respect to processing of key-coded data for scientific purposes.

The risk of harm to individual data subjects arising from scientific uses and disclosures of key-coded data are very minimal. The Article 29 Working Party appeared to recognize this point when it stated in its Working Paper 136 on the concept of 'personal data' (Opinion 4/2007) 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 and ACRO fully agree with this comment and urge that this principle be incorporated into the Directive itself by establishing key-coded data for scientific purposes as a distinct category of data. Without incorporation of this principle into the EU Data Protection Directive itself, member states will continue to impose requirements applicable to key-coded data for scientific purposes in a disjointed and conflicting manner,³ which is not in patients' best interests.⁴

³ Compare, e.g., the very different treatment of key-coded clinical research data in Spain (under the Farmindustria Code approved by the AEPD) versus Italy (under the Garante Guidelines of 24 July 2008 for Data Processing within the Framework of Clinical Drug Trials).

⁴ Harmonization is also of vital importance with respect to what data elements can be included in a key-coded data set. Currently, local legal requirements in some EU member states permit collection of research subject initials and full date of birth while others prohibit this collection. These data elements can be important in the event of a research subject adverse event to ensure that the patient receives the correct treatments.

Conclusion

IPPC and ACRO appreciate this opportunity to provide further input in response to the Commission's Consultation, particularly as it pertains to the future of research in the European Union. We welcome further dialogue on these critical issues and respectfully request a private meeting with the Commission's Data Protection Unit during this exploratory phase. We would be happy to provide specific legislative proposals for how to amend the Data Protection Directive in accordance with these comments. Thank you in advance for your consideration.

International Pharmaceutical Privacy Consortium

1500 K Street, NW, Suite 1100
Washington, DC 20005
T 202 230 5142 **F** 202 842 8465
www.pharmaprivacy.org

Association of Clinical Research Organizations

818 Connecticut Avenue, NW, Suite 1100
Washington, DC 20006
T 202 464 2310 **F** 202 464 2309
www.acrohealth.org

DC01/ 2532035.3