



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](http://www.pharmaprivacy.org)

---

October 26, 2011

**VIA FEDERAL E-RULEMAKING PORTAL**

c/o Jerry Menikoff, M.D., J.D.  
Office for Human Research Protections  
Department of Health and Human Services  
1101 Wootton Parkway, Suite 200  
Rockville, MD 20852

**Re: Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators (Docket no. HHS-OPHS-2011-0005)**

Dear Secretary Sebelius:

The International Pharmaceutical Privacy Consortium (IPPC) is an organization formed in 2002 and comprised of chief privacy officers and other data privacy and security professionals from a number of research-based, global pharmaceutical companies. The IPPC is committed to the promotion of sound policies for the protection of patient privacy and advancement of drug development and treatment. Information concerning IPPC membership and mission is described in Appendix A.<sup>1</sup>

IPPC members sponsor clinical research that is used to support applications to market new drugs. Such research is subject to the Food and Drug Administration regulations governing protection of human subjects. This research is often conducted at institutions that also receive federal funding for research subject to the Common Rule. Many of these institutions voluntarily extend the application of the Common Rule to privately funded research conducted at their institutions. As a result, clinical research on new drugs is often subject to both the FDA regulations as well as the Common Rule.

The IPPC appreciates this opportunity to provide comments on the Advanced Notice of Proposed Rulemaking (ANPRM). Our comments will address the following issues:

- 1) Extension of the Common Rule to all research at a domestic institution that receives some federal funding for research with human subjects;
- 2) Harmonization of the HIPAA Privacy Rule concepts of individually identifiable information, limited data sets, and de-identified information with definitions and concepts in the Common Rule;

---

<sup>1</sup> For further information concerning the IPPC, please visit our website at [www.pharmaprivacy.org](http://www.pharmaprivacy.org). All Appendices referenced in this comment, and additional documents adopted by the IPPC, are publicly available on this website.

- 3) Establishment of mandatory data security and information protection standards based on the HIPAA Security Rule requirements for all studies under the Common Rule that involve identifiable or potentially identifiable data;
- 4) Modification of the categories of research that are exempt from requirements to obtain research subject consent;
- 5) Categorization of all research involving the primary collection of biospecimens as well as storage and secondary analysis of existing biospecimens as research involving identifiable information; and
- 6) Specification that consent for future research would not need to be study-specific and could cover open-ended future research.

**I. Extension of the Common Rule to All Research at a Domestic Institution that Receives Some Federal Funding for Research with Human Subjects.**

***IPPC Recommendation***

The IPPC suggests that rather than extending the application of the Common Rule to privately funded research already subject to FDA human subject research protections, HHS should seek to harmonize the FDA regulations with the Common Rule. The IPPC also supports the incorporation of privacy protections into the Common Rule and FDA regulations and then exempting all human subjects research from HIPAA requirements.

The ANPRM seeks comment on whether the applicability of the Common Rule should be extended to all research that is conducted at a domestic institution that receives some Federal funding for research with human subjects from a Common Rule agency. The IPPC suggests that rather than extending the application of the Common Rule to privately funded research already subject to FDA human subject research protections, HHS should seek to harmonize the FDA regulations with the Common Rule. The application of multiple, overlapping regulations creates confusion for researchers, research sponsors, and the public as to compliance obligations. Researchers should be able to look to a single set of rules to understand their responsibilities. When requirements are spread out among multiple regulations, misunderstandings are more likely to occur. At the same time, participants in research studies should know that they are protected regardless of whether the source of funding is public or private.

In multi-site studies, it adds an unnecessary layer of complexity if some sites are subject to the Common Rule while others are not. The differences between the Common Rule as proposed in the ANPRM and current FDA regulations could lead sponsors to have to maintain different protocols and informed consent forms depending upon whether the site in question is subject to the Common Rule. This is inefficient and will increase overall study costs. Instead of layering different requirements on top of each other, harmonization of federal human subject research protections should be sought.

Harmonization of federal human subject research protections should also include HIPAA requirements. Data privacy and security protections in the biomedical research area should be addressed in a uniform framework for human subject research protections rather than through piecemeal protections enacted under HIPAA or other federal privacy/security legislation that are not focused on the unique needs of researchers. The IPPC supports the incorporation of privacy protections into the Common Rule and FDA regulations and then exempting all human

subjects research from HIPAA requirements. This is consistent with President Obama's January 18, 2011, Executive Order 13563 calling for the "retrospective analysis of rules that may be outmoded, ineffective, insufficient, or excessively burdensome, and to modify, streamline, expand, or repeal them in accordance with what has been learned." It is also consistent with HHS's Plan for Retrospective Review of Existing Rules, which was issued on August 22 pursuant to EO 13563. Further still, it is consistent with recommendations of the Secretary's Advisory Committee on Human Research Protections (SACHRP). Finally, it is consistent with the report of the Institute of Medicine entitled "Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research."

**II. Harmonization of the HIPAA Privacy Rule Concepts of Individually Identifiable Information, Limited Data Sets, and De-identified Information with Definitions and Concepts in the Common Rule.**

***IPPC Recommendation***

The IPPC supports in principle the goal of harmonizing the terms used in the HIPAA regulations with the terms used in the Common Rule. However, the substantive rules that apply to research uses of de-identified information and limited data sets should be far less onerous than the rules governing research uses of fully identifiable data.

The ANPRM seeks comments on whether the use of the HIPAA Privacy Rule's standards for identifiable and de-identified information, and limited data sets, will facilitate the implementation of data security and information protections. The IPPC supports the harmonization of these concepts for purposes of consistency and simplicity. However, the degree of protections required should be commensurate to the identifiability of the information.

In 2004, the Secretary's Advisory Committee on Human Research Protections (SACHRP) recommended that HHS review its HIPAA de-identification standard to more closely align it with the pre-existing Common Rule interpretation of identifiability and to ease the burden on researchers:

The Department should review the standards for de-identification of data in order to reduce the number of data categories that must be eliminated for data to be regarded as de-identified. Among those data categories that should be strongly considered for deletion from the de-identification standards are zip codes, geographic subdivisions, and dates. While the specific addresses of persons should not be included in de-identified information, more general areas of residence, work or origin, may, in fact, be essential to epidemiologic and other studies of, for example, disease incidence. Additionally, most dates, including admission and discharge dates, provide essential endpoints for much research without directly identifying the individual.<sup>2</sup>

<sup>2</sup> See <http://www.hhs.gov/ohrp/sachrp/hipaalettertosecy090104.html>.

The IPPC agrees with SACHRP's conclusion that the HIPAA de-identification safe harbor standard creates problems for researchers with respect to the removal of zip codes, geographic subdivisions, and dates related to the individual. For example, the inclusion of specific dates of birth in records related to infants and young children is necessary for some types of age-related research. Similarly, specific physical location is necessary for site-related health effects research. We also recognize, however, that different definitions of identifiability between the Common Rule and HIPAA rules may create confusion. Therefore, the IPPC supports the harmonization of these terms, provided the rules recognize that the protections appropriate for de-identified data and limited data sets should be far less onerous than the protections required for fully identifiable data. This issue is further addressed in Section IV, below.

### **III. Establishment of Mandatory Data Security and Information Protection Standards Based on the HIPAA Security Rule Requirements for All Studies Under the Common Rule that Involve Identifiable or Potentially Identifiable Data.**

#### ***IPPC Recommendation***

Strong technical, physical, and administrative security safeguards should apply to identifiable data used in research, provided such safeguards are flexible and scalable to the size of the business and scope of risks involved. Similarly, the IPPC supports a general prohibition on the re-identification of de-identified data. We do not support a prohibition on the disclosure of de-identified data to pharmaceutical researchers not subject to the Common Rule as this would seriously impede pharmaceutical research.

The ANPRM proposes to establish mandatory data security standards for all studies under the Common Rule that involve identifiable or potentially identifiable data. Specifically, the ANPRM suggests that for research involving individually identifiable information, biospecimens, or limited data sets, data security standards would require the use of reasonable and appropriate encryption for data maintained or transmitted in electronic form, as well as audit trails and access controls that allow only authorized personnel to have access to the information. Strong physical safeguards would be required for information maintained in paper form. Further, investigators would be required to adhere to breach notification standards modeled on those applied to HIPAA covered entities. For research using limited data sets or de-identified information, investigators would be strictly prohibited from attempting to reidentify the subjects of the information.

Strong technical, physical, and administrative security safeguards should apply to identifiable data used in research, provided such safeguards are flexible and scalable to the size of the business and scope of risks involved. The IPPC agrees that once security safeguards are required, HIPAA covered entities should be permitted to disclose limited data sets to investigators for research purposes without obtaining data use agreements. It makes no sense to require the execution of data use agreements that serve no purpose other than to reiterate regulatory requirements.

The IPPC also supports HHS's proposal to prohibit researchers from re-identifying de-identified data, provided there is a limited carve out for public health safety purposes. Researchers generally have no need, intent or reasonably available means to re-identify data subjects. While we believe the need to re-identify de-identified data for public health safety

purposes is likely extremely rare, we support the inclusion of a limited carve out from the prohibition should the need arise.

The IPPC would not support a prohibition on the disclosure of de-identified data to pharmaceutical researchers not subject to the Common Rule as this would seriously impede pharmaceutical research. Pharmaceutical researchers rely on access to de-identified health information for a variety of types of research, including epidemiological research, and outcomes and effectiveness research. While the costs to society of impeding such research are great, the risk of re-identification of de-identified data is extremely low. Indeed, we are unaware of any examples of the re-identification of de-identified data for a nefarious purpose. De-identified information is far more likely to be re-identified by a computer scientist attempting to prove the ability to re-identify the data than by a medical researcher (because the statistician may have the incentive and requisite experience whereas the medical researcher has neither). Pharmaceutical companies already prohibit researchers working on their behalf from attempting to re-identify de-identified data. As noted earlier, the IPPC supports the harmonization of FDA human subject protection requirements with the Common Rule and believes that the disclosure of data between entities subject to either set of regulations should be permitted.

#### **IV. Modification of the Categories of Research that Are Exempt from Requirements To Obtain Research Subject Consent.**

##### ***IPPC Recommendation***

Given the proposed data security requirements and prohibition on re-identification of data subjects, the risks to individuals of research uses of de-identified data and limited data sets are very small. It may be appropriate for HHS to make a blanket determination that the use of de-identified data and limited data sets meets the criteria for waiver of consent in certain contexts. Nevertheless, whatever HHS decides as to the final content of the revised Common Rule, the IPPC urges the Department not to retrospectively apply the new data security and information protection standards to data and biospecimens collected prior to the implementation of the revised rule.

Under the ANPRM's proposed changes, written consent would not be required to use pre-existing data (i.e., data that were previously collected for purposes other than the currently proposed research study) if the data were originally collected for non-research purposes and the researcher does not obtain information that identifies research subjects or is identifiable. If such data were identifiable (but excluding research using limited data sets), consent would be required. However, if such pre-existing data were originally collected for research purposes, then consent would be required regardless of whether the researcher obtains identifiers (i.e., consent would be required for research using limited data sets as well as even for research involving de-identified data). HHS proposes to apply these changes prospectively to biospecimens and data collected after the effective date of the new rules.

A useful framework for evaluating when subject consent should be required and/or IRB review and approval is to categorize research into several buckets based on the types of risks to subjects. One type of risk relates to the potential for physical harm. The traditional view has been that research that involves the potential for physical harm (e.g., interventional research using a test article) should ordinarily require both the consent of the data subject as well as IRB review and approval. Informational risks can be divided into two separate categories. One type

of informational risk relates to the potential for embarrassment, stigmatization, or discrimination due to the disclosure of private identifiable information. This type of risk can be effectively minimized through implementation of data security safeguards. The traditional view has been that whether consent or IRB waiver of consent is necessary to address this type of informational risk depends on the degree of identifiability of the information.

A second type of informational risk relates to the potential to offend an individual's right of informational autonomy. This is a difficult harm to address because this right is ill-defined.— There is simply not a societal consensus on where such a right begins and ends. As a general matter, most would agree that information that is completely anonymous falls on one end of the spectrum of what information an individual has a right to control. On the other end of the spectrum falls information that identifies the individual. Other factors are also relevant here, however, such as the degree to which the information is already in the public domain and the choices the individual has previously made as to disclosure of the information. In assessing this type of informational risk for purposes of revisions to the Common Rule, it is appropriate for HHS to consider how the law otherwise allows the use of data outside of the research context. In this respect, it is notable that the HIPAA Privacy Rule permits the use and disclosure of de-identified information *for any purpose whatsoever*. This appears to reflect a general view that even though respect for autonomy and individual privacy rights is important, these interests must be balanced with other societal needs for access to health information.<sup>3</sup>

The IPPC respects the view that when data carries a risk of being linked to a specific individual, either that individual's consent should be obtained to use the data or an IRB waiver of consent should be obtained. Considerations in granting a waiver should include the practicability of obtaining consent and the risks to individual subjects of use of the data. We also recognize, however, that in the context of de-identified data or data that only contains limited indirect identifiers like zip codes or dates of birth, it is virtually always impracticable to obtain consent to a secondary use of the data if such consent was not obtained at the time of data collection. Moreover, we recognize that given the proposed data security requirements and prohibition on re-identification of data subjects, the risks to individual subjects of the use of de-identified data or limited data set data are extremely small. Therefore, we believe that it would be appropriate for HHS to make a blanket determination that the use of de-identified data and limited data sets for research purposes meets the criteria for waiver of consent. Such a blanket exemption may be more efficient than requiring case-by-case IRB determinations.

In the ANPRM, HHS proposes to distinguish between data and biospecimens originally collected for research purposes versus data and biospecimens originally collected for non-research purposes. Presumably, the Department's rationale for this distinction is that open-ended consent for future research can be obtained when data/biospecimens are collected for research purposes, but it is much more difficult to obtain consent when the data/biospecimens were collected for non-research purposes. The IPPC agrees that when data/biospecimens are collected for research purposes, this presents an opportunity to obtain general consent for secondary research purposes. Researchers should be encouraged to obtain consent for secondary research when collecting data/biospecimens, to the extent secondary research is contemplated. However, unless HHS agrees to allow broad, open-ended consent for secondary research, there will still be instances in which the consent does not cover all of the secondary

---

<sup>3</sup> TOM L. BEAUCHAMP AND JAMES F. CHILDRESS, PRINCIPLES OF BIOMEDICAL ETHICS 295 (2008).

analyses that researchers wish to conduct. It is simply impossible to foresee all of the potential secondary research uses at the time of data collection. Therefore, even where data/biospecimens were originally collected for research purposes, it may still be appropriate for HHS to make a blanket determination that the use of de-identified data and limited data sets for research purposes meets the criteria for waiver of consent.

Whatever HHS decides as to the final content of the revised Common Rule, the IPPC urges the Department not to retrospectively apply the new data security and information protection standards to data and biospecimens collected prior to the implementation of the revised rule. It is impractical (and in most circumstances, likely *impossible*) for researchers to obtain consent for research using de-identified data, limited data sets, and biospecimens collected for research purposes if such consent was not obtained at the point of data/sample collection. If the rules were retrospectively applied to such data/samples, either IRB waivers would need to be sought or the data/samples would need to be destroyed.

**V. Categorization of All Research Involving the Primary Collection of Biospecimens as well as Storage and Secondary Analysis of Existing Biospecimens as Research Involving Identifiable Information.**

***IPPC Recommendation***

Where researchers are prohibited by law or contract from identifying biospecimens and from sharing the specimens for non-research purposes, the risk of identification is low. The degree of protections required for research using biospecimens should be commensurate to the risk of identification.

HHS notes in the ANPRM that DNA extracted from de-identified biospecimens can be sequenced and analyzed with the results sometimes being linked to other available data that may allow a researcher to identify the persons whose specimens are being studied. The ANPRM seeks comments on whether a human biospecimen should be considered identifiable in and of itself.

Data derived from biological samples can be identifiable or non-identifiable, just as other personal health data can be. Genetic data are non-identifiable unless a reference database or similar available record source exists that links them to individual identities and this is accessible to the researcher. Where researchers are prohibited by law or contract from identifying biospecimens and from sharing the specimens for non-research purposes, the risk of identification is low. Moreover, researchers generally have no incentive (let alone a readily available means) to link biospecimen samples to individual identities. The degree of protections required for research using biospecimens should be commensurate to the risk of identification.

For research using directly identifiable biospecimens, general consent should provide a permissible basis for such research. This issue is further addressed in Section VI, below. As an alternative basis for such research, the IPPC believes that IRBs should retain the authority to evaluate the risk of embarrassment, stigmatization, and discrimination associated with the research, as well as to determine that the benefits of the research outweigh individual informational autonomy rights. This issue was addressed in Section IV, above.

**VI. Specification that Consent for Future Research Would Not Need To Be Study-Specific and Could Cover Open-Ended Future Research.**

***IPPC Recommendation***

The IPPC supports permitting general consent for future research on biospecimens and data. Examples of an acceptable level of detail for such consents include permitting research concerning the same test article, permitting research concerning the same disease state or condition, and permitting research concerning related diseases and conditions.

The IPPC supports permitting general consent for future research on biospecimens and data. It is often impossible at the time of the initial biospecimen/data collection to understand the range of analyses that researchers may wish to perform on such biospecimens/data in the future. Nevertheless, examples that we believe offer an acceptable level of detail for such consents include permitting research concerning the same test article, permitting research concerning the same disease state or condition, and permitting research concerning related diseases and conditions. Researchers should be given the flexibility to decide how they wish to structure consent documents so as to best convey informational risks and options regarding future research.

It is impossible to anticipate all the different sensitivities that individuals may have to different types of research. To the extent that HHS believes that certain types of research may pose greater risks to individuals or raise more acute sensitivities than other types of research, we believe that such risks/sensitivities could be addressed in the information provided in the consent. For example, a general consent for future research could indicate whether the future research to be conducted may include biomedical research, social sciences research, or other types of research. To the extent HHS believes that research involving certain types of health information or research conducted for certain purposes are likely to raise more sensitivities than other types of research, the potential for these types of research activities could also be explained generally in the consent. However, we caution against a long list of required elements or statements as such requirements inevitably increase the length and complexity of the consent form.

---

We thank you for your consideration of our comments and would welcome the opportunity to discuss these issues with you.

Please do not hesitate to contact us with any questions.

Sincerely,



Mary Devlin Capizzi  
Secretariat and Legal Counsel

## APPENDIX A: INTERNATIONAL PHARMACEUTICAL PRIVACY CONSORTIUM

<b>MEMBERS</b>	<p>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:</p> <table border="0"> <tr> <td>w Abbott Laboratories</td> <td>w Merck &amp; Co.</td> </tr> <tr> <td>w AstraZeneca</td> <td>w Novartis</td> </tr> <tr> <td>w Baxter International</td> <td>w Pfizer Inc.</td> </tr> <tr> <td>w Bristol-Myers Squibb</td> <td>w Genentech / Roche</td> </tr> <tr> <td>w Eli Lilly and Company</td> <td>w Sanofi-aventis</td> </tr> <tr> <td>w GlaxoSmithKline</td> <td>w Takeda Pharmaceuticals</td> </tr> </table>	w Abbott Laboratories	w Merck & Co.	w AstraZeneca	w Novartis	w Baxter International	w Pfizer Inc.	w Bristol-Myers Squibb	w Genentech / Roche	w Eli Lilly and Company	w Sanofi-aventis	w GlaxoSmithKline	w Takeda Pharmaceuticals
w Abbott Laboratories	w Merck & Co.												
w AstraZeneca	w Novartis												
w Baxter International	w Pfizer Inc.												
w Bristol-Myers Squibb	w Genentech / Roche												
w Eli Lilly and Company	w Sanofi-aventis												
w GlaxoSmithKline	w Takeda Pharmaceuticals												
<b>MISSION</b>	<p>The IPPC was formed in 2002 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.</p>												
<b>GOALS</b>	<p>The IPPC goals are to:</p> <ul style="list-style-type: none"> <li>w Engage government and stakeholders in the biomedical research and healthcare communities in a constructive dialogue on significant issues of privacy and data protection.</li> <li>w Serve as a resource for sound analyses of privacy and data protection requirements and compliance tools tailored to the pharmaceutical industry.</li> <li>w Serve as a forum for industry dialogue and promote responsible privacy and data protection practices.</li> <li>w Promote consistent privacy and data protection standards that can be achieved on a worldwide basis.</li> </ul>												
<b>SCOPE OF ACTIVITIES</b>	<p>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:</p> <table border="0"> <tr> <td>w Biomedical research</td> <td>w Market research</td> </tr> <tr> <td>w Pharmacovigilance</td> <td>w Human resources programs</td> </tr> <tr> <td>w Sales and marketing</td> <td>w Other corporate programs</td> </tr> </table>	w Biomedical research	w Market research	w Pharmacovigilance	w Human resources programs	w Sales and marketing	w Other corporate programs						
w Biomedical research	w Market research												
w Pharmacovigilance	w Human resources programs												
w Sales and marketing	w Other corporate programs												