



# MEDICAL RESEARCH LAW & POLICY



## REPORT

Reproduced with permission from Medical Research Law & Policy Report, Vol. 3, No. 7, 04/07/2004, pp. 271-276. Copyright © 2004 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

### Transfer of Clinical Research Data from the European Union to the United States

By STEPHEN W. BERNSTEIN, RALF WEISSER,  
ANDREAS BAUER, AND ROHAN MASSEY

#### 1. Introduction

**F**or U.S. pharmaceutical companies, clinical trials undertaken in Europe offer numerous advantages, such as high-quality performance, low liability risks, and a sensible, harmonized legal framework. For these reasons, an ever growing number of U.S. pharmaceutical companies are conducting clinical trials in the European Union (“EU”). It is likely that this number will continue to increase following the accession to the EU of 10 more states, mainly Eastern European, on May 1, 2004. The harmonization of standard rules governing clinical trials in the EU has greatly facilitated the performance of cross-border studies. In particular, the international Guideline on Good Clinical Practice (“ICH GCP”),<sup>1</sup> which sets out standards that are accepted by

<sup>1</sup> International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use, Guideline for Good Clinical Practice, E6, adopted by the EU Committee for Proprietary Medicinal Products (July 1996, issued as CPMP/ICH/135/95/Step5, and Explanatory Note and Comments, issued as CPMP/768/97). Adopted in the United States by the Food and Drug Administration (published in the

*Stephen W. Bernstein and Ralf Weisser are partners with the international law firm of McDermott, Will & Emery, in Boston and Munich, respectively.*

*Andreas Bauer and Rohan Massey are associates with McDermott, Will & Emery, in Munich and London, respectively.*

the U.S. Food and Drug Administration (“FDA”) as well as by the European regulatory authorities. Despite this growing conformity, substantive differences between EU member states remain when it comes to data privacy requirements.

From the U.S. perspective, the main difficulty seems to be the transfer of personal data from the EU to the United States. This article illustrates methods that can be used to assess the legal compliance of data transfer to the United States against the background of sometimes different national regulations within the EU.

#### 2. EU Privacy Legislation

At an EU level, the starting point for a review of the legal requirements is the EU directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 95/46/EC) (“Data Protection Directive”).<sup>2</sup> EU directives differ from national laws: they do not legally bind national citizens but instead are addressed to the EU member states. A directive is only binding on the result to be achieved, but leaves the precise choice of form and method to individual national authorities.<sup>3</sup> After a directive has been enacted, each member state is required to pass national legislation necessary to ensure local compliance with the directive. Therefore, it is not the directive but rather the national laws of the member state that specify the national requirements. Despite the fact that each member state is implementing the same directive, there often are slight differences in the wording and substance of each national law. In some cases,

*Federal Register*, Vol. 62, No. 90, May 9, 1997, pp. 25691-25709).

<sup>2</sup> *Official Journal of the European Communities (O.J.)* L 281, Nov. 23, 1995, pp. 31-50.

<sup>3</sup> Treaty establishing the European Community, Art. 249, paragraph 4 (O.J. C 325, Dec. 24, 2002, p. 33).

the directive itself may leave some discretion to national legislators. For example, Art. 26 of the Data Protection Directive allows the transfer of personal data to countries outside of the EU “save where otherwise provided by domestic law governing particular cases.”

As it is the local law of the member state, including its derogation or variations from the directive, that must be observed, one cannot rely only on the Data Protection Directive for definitive guidance. A review of the domestic privacy laws in each member state in which a clinical trial will take place always will be necessary. Therefore, national data protection regulation is the second legal source. An example of these national laws and their interaction with the Data Protection Directive is the German Federal Data Protection Act,<sup>4</sup> the U.K.’s Data Protection Act 1998, and Italy’s Protection of Individuals and Other Subjects with regard to the processing of Personal Data Act No. 675 of Dec. 31, 1996.

When undertaking multi-jurisdictional clinical trials within the EU, harmonized but nevertheless substantially different privacy laws must be observed. Fortunately, there is some facilitation: Art. 4 of the Data Protection Directive stipulates that each member state apply its national provisions only if the processing is carried out by a data controller’s establishment (office rooms) in the respective member country.<sup>5</sup> In reverse, the data controller must observe the legislation only of those member countries in which it is located. As a consequence, for example, a Dutch data controller with German-based offices collecting data in Germany must observe the German Federal Data Protection Act. However, the same Dutch data controller is not bound by the German privacy law if it does not have any office rooms in Germany but carries out its activities from Dutch territory. In this instance the data controller is bound only by Dutch privacy law.

The Data Protection Directive and legislation implementing it in the member states constitute the primary legal regulation of data privacy in the EU. However, there also are specific rules from other areas of law that may stipulate privacy requirements, such as some national drug laws (e.g., German Drug Act) and each member state’s law on professional secrecy.<sup>6</sup>

It also should be noted that a new EU directive on clinical trials (“Clinical Trials Directive”) has been enacted,<sup>7</sup> which member states must implement by May 1, 2004. The national laws regulating clinical trials of most member states will be amended in the near future to accommodate these new administrative requirements associated with the conduct of clinical trials. However, because the Clinical Trials Directive does not directly affect or limit the provisions of the Data Protection

Directive,<sup>8</sup> and instead comprise an additional set of requirements, it is unlikely that the national legislation regarding data privacy itself will change.

### 3. The Scope of the Data Protection Regulation

#### a. What data are concerned?

The Data Protection Directive, and accordingly, the national privacy laws of the EU member states, protect a natural person’s “right to privacy with respect to the processing of personal data.”<sup>9</sup> Therefore, the first issue that must be addressed when undertaking clinical trials within the EU is whether or not the data to be collected will be “personal data.” Personal data means any information relating to an identified or identifiable person.<sup>10</sup> The data collected in clinical trials are likely to be personal data. Moreover, any data relating to a person’s health must be treated as “sensitive” and will be subject to even more strict regulation than personal data.<sup>11</sup> Unlike the United States’ Health Insurance Portability and Accountability Act (“HIPAA”), which regulates types of entities—health care providers that conduct electronic transactions, health plans, and health care clearinghouses—the Data Protection Directive is aimed at types of data, namely “personal data.” As such, the directive is significantly broader than HIPAA both in terms of data type and parties regulated.

In most clinical studies the data are not retained in the form that they are collected. Usually the investigator assigns each trial subject a reference number, the so-called subject identification code (“SIC”). The SIC, as defined by ICH GCP, is a unique identifier assigned by the investigator to each trial subject as a means of protecting the subject’s identity. In general, the SIC is used for reporting trial-related data.<sup>12</sup> For example, case report forms (“CRFs”) from clinical trials carry only this SIC number and not the subject’s identity details. The benefit of this approach is that any person processing CRFs, without the key for unblinding the SIC, would not be deemed to be processing personal data because the data contained in the CRFs cannot be matched to a specific subject. However, certain persons involved in a clinical trial will have direct access to the personal data.<sup>13</sup> Direct access means that an individual can review source documents, such as the patient record, which contain personal data identifying the data subject. Any person that has direct access will be deemed to be working with personal data. Individuals who normally would fall into this category include staff members of foreign and national regulatory authorities, and monitors or auditors working for the clinical research organization (“CRO”), or the sponsor of a particular study.

Where an individual acts in the course of employment, the employee’s knowledge will be attributed to the employing entity. This can create an anomalous result whereby some sponsor’s employees use blinded CRFs but the sponsor nevertheless is deemed to be processing personal data because some of its other employees (for example, monitors) have direct access and are

<sup>4</sup> “Bundesdatenschutzgesetz” of Dec. 20, 1990, in the version published in *The German Federal Law Gazette (Bundesgesetzblatt (BGBl.))*, Part I, Jan. 14, 2003, p. 66.

<sup>5</sup> Within the meaning of the directive, an establishment implies the existence of office rooms, whereas the legal form of the establishment, whether simply a branch or a subsidiary, as a separate legal entity is not decisive. See Data Protection Directive, Recital 19.

<sup>6</sup> See, e.g., Bavarian Occupational Regulations for Physicians, Sec. 9.

<sup>7</sup> Directive 2001/20/EC of April 4, 2001, on the approximation of the laws, regulations, and administrative provisions of member states relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use (O.J. L121/34, May 1, 2001).

<sup>8</sup> See Clinical Trials Directive, Recital 17.

<sup>9</sup> Data Protection Directive, Art. 1, no. 2.

<sup>10</sup> Data Protection Directive, Art. 2, lit. a.

<sup>11</sup> See Data Protection Directive, Art. 8, paragraph 1.

<sup>12</sup> See ICH GCP, definition No. 1.68.

<sup>13</sup> See ICH GCP, definition No. 1.21.

able to trace the identity of a patient from the SIC. In addition, there is no generally accepted EU standard for safe deidentification.<sup>14</sup>

However, the U.S. Department of Commerce “Safe Harbor Privacy Principles” and associated Frequently Asked Questions (“FAQ”), which have been adopted by the EU (see discussion of safe harbor principles below), consider coded clinical data not to be personal data.<sup>15</sup> This assessment is somewhat superficial and does not take into account the various access rights of data controllers’ employees. The ability to trace a trial subject’s identity makes it necessary to qualify blinded data from a study as personal data under the meaning of the Data Protection Directive.<sup>16</sup> Therefore, at least outside of the narrow scope of the FAQs, a data controller employing people with direct access to the patients’ records typically will be deemed to be processing personal data, and thus subject to EU data protection compliance requirements.

### *b. Who must comply with EU data protection legislation?*

In general, the data protection requirements bind every person or body that processes personal data. Therefore, any investigator, sponsor, or CRO is required to observe the relevant privacy requirements. As discussed above and in stark contrast with HIPAA’s requirements, it does not make any difference whether or not a person or body is a health care provider or exchanges information with a health plan or health insurance provider.

Among the parties that are regulated, there is only one specific category. The Data Protection Directive introduces the idea of a “data controller.” The data controller is a natural or legal person who or which, alone or jointly with others, determines the purposes and means of processing personal data. In the Data Protection Directive, the data controller is distinguished from the “data processor,” a natural or legal person who or which processes personal data on behalf of the controller. The implications of this characterization in clinical trials as well as in the context of database research are far-reaching.

In most clinical trials there are three key players: the sponsor, the CRO, and the investigator. Assuming personal data are collected, the sponsor always will be a data controller, because it is responsible for designing the study and, therefore, determines the purpose of the processing of the data. The CRO also often will be a data controller because it determines the means of processing using its own processing systems (In cases

where the data controller is located in the United States, a CRO based in Europe by legal necessity will be a data controller.).<sup>17</sup> However, whether or not the investigator is deemed to be a data controller will be very fact-specific and requires analysis of the applicable facts and circumstances. On the one hand, it can be argued that the investigator merely is collecting or processing personal data on behalf of the CRO or the sponsor. On the other hand, if one compares the investigator with typical data processors such as data processing service centers, it is obvious that the investigator is significantly more independent from the data controller (sponsor or CRO). In particular, the investigator is bound by even more specific rules such as those governing professional secrecy. As a result, the investigator also may be deemed to be a data controller.

A data controller must notify the responsible supervisory authorities of the member state in which it is collecting data of its processing procedures.<sup>18</sup> Unfortunately, despite the goal of harmonization, each member state has framed its own individual administrative responsibilities quite differently. In some more “centralized” countries such as the United Kingdom or France, there is a single authority that is responsible for regulating the entire territory. In federal countries like Germany and Austria, a more sectorial or regional approach has been adopted, with each state having its own competent supervisory authority. Thankfully, in most instances, once the correct competent supervisory authority has been identified, notification is neither complicated nor expensive. In the United Kingdom, for example, annual notification of the Information Commissioner’s Office, as required by the Data Protection Act 1998, can be completed online and costs £35 (\$50).<sup>19</sup> According to Art. 19 of the Data Protection Directive, the information to be given includes at least the name and address of the data controller, the purpose for the processing, the category of the data subjects, and the category of data relating to them. For example, a CRO would note that it collects health data from participants in a clinical trial for the purpose of clinical research. In addition, the data controller must provide the supervisory authority with information about the categories of recipients to whom the data might be disclosed; any proposed transfers of data to third countries outside the EU,<sup>20</sup> for example, to sponsors in the United States; and the measures taken to ensure security of processing.

## **4. Key Problem: Transfer of Personal Data to the United States**

To reduce the risk of regulatory difficulties, all data controllers should comply with the general rules of good clinical practice, process personal data carefully, and use state-of-the-art privacy protection methods and

<sup>14</sup> In contrast, the HIPAA privacy regulations include two very specific methods of deidentification. See 45 C.F.R. § 164.514, which includes a statistical method for deidentification and a so-called “safe harbor” method of deidentification that requires the elimination of 18 specific categories, including birth dates (not year) and dates of service.

<sup>15</sup> See FAQ 14, seventh answer (O.J. L 215/24, Aug. 25, 2000) (FAQ 14 is available at <http://www.export.gov/safeharbor/FAQ14PharmaFINAL.htm>). More information on EC deliberations concerning the safe harbor privacy principles is available at [http://europa.eu.int/comm/internal\\_market/privacy/adequacy\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm).

<sup>16</sup> For discussion of the key role of tracing back, see also, Beach/Strehlow, “Avoiding Contractual Pitfalls in International Clinical Trials,” 2 *Med. Res. Law & Policy Rep.* 745, 747, 10/15/03.

<sup>17</sup> For Germany, see Gola/Schomerus, *Bundesdatenschutzgesetz Kommentar*, 7th ed., Munich 2002, Sec. 3 BDSG, 53.

<sup>18</sup> Member states may make some exemptions; see Data Protection Directive, Art. 18. However, they rarely apply with respect to clinical trials.

<sup>19</sup> See <http://www.dataprotection.gov.uk>.

<sup>20</sup> The additional member states of the European Economic Area, or EEA (The Principality of Lichtenstein, Iceland, and Norway), are put on par with the EU member states. However, in order to simplify matters “EU” is used in this article instead of “EEA.”

technology (which will need to be updated at regular intervals to keep up with technological developments). However, there are some important issues that U.S.-based sponsors and/or CROs need to be aware of concerning the transfer of personal data collected during a clinical trial in Europe to the United States.

The transfer of data across member states of the EU is quite simple: the same rules apply as govern domestic transfer within a member state itself. Therefore, a transfer of personal data between Munich and Berlin does not legally differ from a transfer from Munich to London. However, different rules apply to the transfer of personal data to countries outside of the EU, so-called third countries. According to Art. 25, paragraph 1, of the Data Protection Directive, a data controller may only transfer data to a third country if this receiving third country ensures an “adequate level of protection.” What is an adequate level of protection?

The directive does not list countries that are deemed “adequate.” Instead, it provides criteria about how to determine the adequacy of the level of protection. The criteria address the rules of law, both general and sectorial, in force in the third country as well as the professional rules and security measures that are complied with in the third country. The EU Commission (the “Commission”), as the administrative body of the EU, can determine that a third country has an “adequate” level of protection by reason of either its national laws or of international commitments it has entered into.<sup>21</sup> These decisions of the Commission bind the EU member states. The Commission so far has recognized Argentina,<sup>22</sup> Canada,<sup>23</sup> Guernsey,<sup>24</sup> Hungary,<sup>25</sup> and Switzerland<sup>26</sup> as providing adequate protection.

Surprisingly, the United States has not been deemed to have an “adequate” level of protection. This is due to the sectorial and self-regulatory approach to privacy protection favored by the United States, as opposed to the EU’s blanket legislation approach.<sup>27</sup> Even with HIPAA, which itself is relatively narrow in the scope of who it regulates, the U.S. regulatory scheme has not been deemed adequate by European authorities. Nevertheless, these different approaches do not mean that a transfer of personal data from European countries to the United States is impossible. On the contrary, there are a number of ways in which the smooth and legal transfer of personal data from the EU to the United States can be achieved.

<sup>21</sup> Data Protection Directive, Art. 25, paragraph 6.

<sup>22</sup> Decision of the Commission C (2003) 1731 of June 30, 2003.

<sup>23</sup> Decision of the Commission 2002/2/EC of Dec. 20, 2001 (O.J. L 2/13, Jan. 4, 2002).

<sup>24</sup> Decision of the Commission 2003/821/EC of Nov. 21, 2003 (O.J. L 308/27, Nov. 25, 2003); the Bailiwick of Guernsey is one of the dependencies of the British Crown (being neither part of the United Kingdom nor a colony) and therefore is considered as a third country by the EU Commission.

<sup>25</sup> Decision of the Commission 2000/519/EC of July 26, 2000 (O.J. L 215/4, Aug. 25, 2000).

<sup>26</sup> Decision of the Commission 2000/518/EC of July 26, 2000 (O.J. L 215/1, Aug. 25, 2000).

<sup>27</sup> See Safe Harbor Privacy Principles, 1st paragraph (O.J. L 215/10, Aug. 25, 2003).

## 5. Silver Bullet: Proper Informed Consent—No Safe Harbor Necessary

### a. Safe harbor

To minimize the effects of the United States not satisfying the EU’s adequacy criteria, the Commission agreed to recognize the “Safe Harbor Privacy Principles” (the “Principles”) issued July 21, 2003, by the U.S. Department of Commerce. The Principles ensure an adequate level of protection for personal data transferred from the EU to the United States.<sup>28</sup> Subject to compliance with the Principles, a transfer of personal data from the EU to the United States is as simple as it is within the EU.

In order to benefit from the safe harbor, a U.S. organization has to meet two conditions: first, it must publicly disclose its commitment to comply with the Principles, and second, the organization must be subject to the statutory powers of a U.S. government body<sup>29</sup> that is empowered to sanction the organization if it fails to comply with the Principles.<sup>30</sup>

To disclose its commitment, an organization annually must notify the U.S. Department of Commerce of its compliance with the Principles. This is done by means of a self-certification letter, which is then made publicly available by Commerce in its listing of all organizations participating in the safe harbor scheme.<sup>31</sup>

There are seven issues in the Principles as follows: notice, choice, onward transfer, security, data integrity, access, and enforcement.<sup>32</sup> For any organization considering agreeing to the safe harbor mechanism, “enforcement” is probably the most important issue of the Principles and the one that needs most clarification. Enforcement within the sense of the Principles is based on three requirements:

- The organization joining must establish readily available and affordable independent recourse mechanisms by which individual complaints are investigated and resolved.
- The organization must introduce follow-up procedures to verify that its publicly declared and asserted privacy practices are duly implemented and observed.
- The organization must commit itself to rigorous sanctions in case of failure to comply with the Principles.

The safe harbor is not a burden-free panacea. There are significant procedures that must be undertaken in initial implementation of the Principles. Furthermore, onerous ongoing obligations must be observed, such as the requirement that an organization may need to separate personal data of European origin from U.S. domestic data. For this reason, careful consideration should

<sup>28</sup> Decision of the Commission 2000/520/EC of July 26, 2000, Art. 1, paragraph 1 (O.J. L 215/7, Aug. 25, 2000).

<sup>29</sup> Up to now, the Commission has recognized the U.S. Federal Trade Commission, on the basis of its authority under Section 5 of the Federal Trade Commission Act, and the U.S. Department of Transportation, on the basis of its authority under 49 U.S.C. § 41712.

<sup>30</sup> Decision of the Commission 2000/520/EC of July 26, 2000, Art. 1, paragraph 2 (O.J. L 215/7, Aug. 25, 2000).

<sup>31</sup> The list is available at <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list>.

<sup>32</sup> Further information on the Principles is available at <http://www.export.gov/safeharbor>.

be given to the overall impact on a business before agreeing to abide by the safe harbor.<sup>33</sup>

As a consequence of these burdens, many U.S. companies have been reluctant to join the safe harbor scheme. As of Feb. 1, 2004, the list maintained by the Department of Commerce named approximately 450 organizations. This is a rather small number when compared to the many thousands companies in the United States that receive personal data from within the EU.

### b. Model clauses

A second mechanism for legal compliance when transferring personal data from the EU is covered by Art. 26, paragraph 2, of the Data Protection Directive. This provision enables a data controller to transfer data to third countries if the data controller utilizes adequate safeguards with respect to privacy protection, such as the use of "appropriate contractual clauses." The Data Protection Directive does not define "appropriate," but the Commission can officially determine that certain "standard" contractual clauses are appropriate within the sense of the directive.<sup>34</sup> Such a decision is binding on member states. So far, the Commission has recognized one set of standard contractual clauses stipulating the transfer from a European-based data controller to a data controller located in a third country.<sup>35</sup>

According to clause 5 of these recognized standard contractual clauses, the data importer (for example, a U.S.-based sponsor) enters into numerous obligations. First of all, the data importer must warrant to process personal data in accordance with the data protection principles set forth in an appendix to the standard contractual clauses (clause 5, paragraph b). This appendix includes obligations with regard to the purpose of processing, the quality and proportionality of data processed, the transparency and security of processing, and the data subject's right of access, rectification, erasure, and blocking of data. Where data concerning health (for example, data collected in a clinical trial) are processed, additional safeguards must be in place, such as strong encryption for transmission or keeping a record of access. As an additional obligation under clause 5, the data importer must submit a list of the data processing facilities used for audit by the data exporter (for example, an investigator located in the EU) or by an independent inspection body.

Furthermore, these recognized standard contractual clauses require the establishment of an agreement between the data exporter and the data importer in favor of the data subject as third party beneficiary. As a result, the data subject can claim damages for violation of his or her privacy rights. Since the data exporter and the data importer must agree that they will be jointly and severally liable for damages suffered by the data subject (clause 6), the U.S.-based entity may be liable for violations committed by its European counterpart.

In conclusion, the standard contractual clauses offer an additional way for EU data controllers to transfer

personal data to the United States. Nevertheless, they also create significant obligations and liability. Therefore, these clauses should not be adopted without considering the specifics of each clause, the implications for the parties involved, and the ability of the parties to maintain compliance.

### c. Codes of conduct

A further means of establishing adequate safeguards that will allow a transfer to data importers outside of the EU are "codes of conduct."<sup>36</sup> Such codes must be authorized by national supervisory authorities not only when they are initially established, but also whenever they are revised. The effect of this approach is that codes are a highly regulated and relatively inflexible method of attaining a legally compliant transfer of personal data, particularly in situations where the type of data collected or the data processing methods may vary.

### d. Data subject consent

The final method for ensuring legally compliant transfers of personal data to third countries is to obtain the data subject's consent. Because the ICH GCP guidelines and the corresponding national drug regulations require informed consent for compliance in their own right, it should be a matter of course to obtain data subjects' consent in clinical trials.<sup>37</sup>

Art. 26 of the Data Protection Directive allows a transfer of personal data to an "unsafe" third country if the data subject unambiguously has given his or her consent. The directive defines the subject's consent as "any freely given specific and informed indication of the data subject's wishes by which the subject signifies his or her agreement to personal data being processed."<sup>38</sup> From these provisions, one can derive the requirements for an appropriate consent.

The data subject must be given all relevant and necessary information prior to obtaining consent. The information to be provided by the data controller includes a contact name and address, the purpose of the collection and processing, as well as the purpose of the transfer.<sup>39</sup> As the consent must be specific, the purpose should be carefully described in terms that ensure clarity and are not too broad or general. However, as any change of purpose requires a new consent, care must be taken to ensure the wording of the consent covers all anticipated use of the data, both present and future.<sup>40</sup>

The data subject also must be informed about the category of data to be transferred (for example, clinical

<sup>36</sup> See, e.g., German Federal Data Protection Act, Sec. 4c, paragraph 2.

<sup>37</sup> See the detailed requirements for the informed consent of trial subjects set forth by ICH GCP No. 4.8, and, as an example of such requirements in national drug laws, German Drug Act, Section 40.

<sup>38</sup> Data Protection Directive, Art. 2(h).

<sup>39</sup> Ehrmann/Helfrich, *EG Datenschutzrichtlinie*, Cologne 1999, Data Protection Directive, Art. 2, 70.

<sup>40</sup> Recently, there has been discussion among U.S. research centers, the National Institutes of Health, and the Department of Health and Human Services Office for Civil Rights regarding the degree of specificity required in a HIPAA-compliant authorization for release of information, particularly with regard to data repositories containing data received that may be used later for research not specified in the original authorization. This dialogue is useful in the context of both HIPAA and EU data protection. See <http://privacyruleandresearch.nih.gov/pdf/>

<sup>33</sup> Räther/Seitz, *Multimedia und Recht (MMR)* 2002, 425, 429.

<sup>34</sup> Data Protection Directive, Art. 26, paragraph 4.

<sup>35</sup> Decision of the Commission 2001/497/EC of June 15, 2001 (O.J. L 181/19, July 4, 2001); the second set of clauses under 2002/16/EC of Dec. 27, 2001 (O.J. L 6/52, Jan. 10, 2002) stipulates the transfer to a processor (agent) in a third country and is of no relevance in this context.

health data). The identities of the recipients in the third country, such as the regulatory authorities or the sponsor, must be disclosed as well.<sup>41</sup> In circumstances where personal data are sent to a country where privacy protection is not recognized as adequate (for example, the United States), the data subject must be informed that the privacy laws in the receiving country are not as strict as they are in his or her home country.<sup>42</sup>

The consent should be given “unambiguously.” This does not per se mean that the data subject must provide a written consent,<sup>43</sup> although the ICH GCP guidelines,<sup>44</sup> and some national laws,<sup>45</sup> do require a written consent. To limit potential risk of noncompliance, it is strongly recommended that data controllers obtain a written consent from each data subject. Because the informed consent form for the participation in the study must be provided in writing and must be signed by the data (and trial) subject anyway, written consent usually does not create much additional effort.

According to ICH GCP guidelines, the requirements of the Data Protection Directive regarding consent can be incorporated into the data subject’s consent to participate in the clinical trial. Nevertheless, the consent to transfer data to an “unsafe” third country, albeit contained in the same document as the clinical trial informed consent, should be clearly distinguishable from the trial participation language, for example, printed in bold type or included in a separate box.

The consent to the transfer should be obtained prior to the collection of data. While some EU member states, such as the United Kingdom and Belgium, permit a retroactive consent, other member countries do not.<sup>46</sup> In any case, failing to prepare and obtain a compliant consent (at the outset or retroactive where allowed) can have significant regulatory implications, including fines and cessation of future data collection. For example, according to German law, a data controller can be punished with a fine up to 250,000 Marks (\$300,000)<sup>47</sup> or even can be imprisoned for up to two years.<sup>48</sup> In addi-

tion, for example, according to Belgian law, a court may order to publish the judgment, may confiscate the personal data collected, and may enjoin the data controller from managing any personal data for a period of up to two years.<sup>49</sup>

Of all the means of transferring data from the EU to the United States, consent is the most likely pathway to be used. While ordinary businesses could have problems obtaining (written) data protection consent, a clinical investigator must ask the trial subject for such consent to participate in the study anyway. Thus, only incremental additional effort is needed to obtain this “second” kind of consent (most likely within the same informed consent document) for permission to transfer data to third countries, particularly those countries not deemed “safe” by the European Commission. Furthermore, by participating in a clinical trial, research subjects run the (in most cases relatively small) risk of adversely affecting their health. Therefore, most clinical trial subjects likely will consent to the transfer of personal data to a third country like the United States. For the trial subject, the danger involved with data transfer is likely to seem fairly small compared to the significance of the health risks associated with the study.<sup>50</sup>

## 6. Conclusion

This article illustrates that personal data may be conveniently and legally transferred from the EU to the United States, and that it is not necessary to comply with the safe harbor framework. Informed consent often is the preferable route. Data protection issues, therefore, should not prevent U.S. sponsors from reaping the benefits of undertaking clinical trials in Europe. Nevertheless, given the patchwork of individual country requirements even within the EU, care must be taken to ensure compliance with both the Data Protection Directive as well as its specific application within each of the countries from which data are derived. Once these are identified and the flow of data analyzed, registration and development of compliant consent forms can be relatively straightforward. Failure to conduct this review, however, can have serious implications for the pending clinical trial, data collection and analysis, and future research within the affected countries.

ment, or with the intention of enriching himself or another person (German Federal Data Protection Act, Sec. 44, paragraph 1).

<sup>49</sup> Belgian Law of Dec. 8, 1992, on Privacy Protection in Relation to the Processing of Personal Data (as modified by the law of Dec. 11, 1998 implementing Directive 95/46/EC), Art. 40 and 41.

<sup>50</sup> A “chilling effect” on patient enrollment as described by Beach/Strehlow in “Avoiding Contractual Pitfalls in International Clinical Trials,” (2 *Med. Res. Law & Policy Rep.* 745, 10/15/03), cannot be confirmed from a European perspective. Trial subjects generally are well-informed by the investigators and do not shy away from signing consent forms. These data protection consents also are fully recognized as “freely given” by the EU member states, especially in view of Art. 26 of the Data Protection Directive.

clin\_research.pdf, and [http://privacyruleandresearch.nih.gov/pdf/research\\_repositories\\_final.pdf](http://privacyruleandresearch.nih.gov/pdf/research_repositories_final.pdf).

<sup>41</sup> See Art. 29 Data Protection Working Party Recommendation 2/2001, p. 5 (available at [http://www.europa.eu.int/comm/internal\\_market/privacy/workinggroup/wp2001/wpdocs01\\_en.htm](http://www.europa.eu.int/comm/internal_market/privacy/workinggroup/wp2001/wpdocs01_en.htm)); and, as an example of a national law requirement under the German Federal Data Protection Act, Simitis/Simitis, *Kommentar zum Bundesdatenschutzgesetz*, 5th ed. Baden-Baden 2003, Sec. 4c, 9.

<sup>42</sup> Art. 29 Data Protection Working Party Recommendation 2/2001, p. 5.

<sup>43</sup> Ehrmann/Helfrich, *EG Datenschutzrichtlinie*, Cologne 1999, Art. 26, 7.

<sup>44</sup> ICH GCP No. 4.8.10(n).

<sup>45</sup> See, e.g., German Federal Data Protection Act, Sec. 4a.

<sup>46</sup> See, e.g., German Federal Data Protection Act, Sec. 4a; Simitis/Simitis, *Kommentar zum Bundesdatenschutzgesetz*, 5th ed., Baden-Baden 2003, Sec. 4c, margin note 9.

<sup>47</sup> German Federal Data Protection Act, Sec. 43, paragraph 2, no. 1, and paragraph 3.

<sup>48</sup> Imprisonment, however, is imposed only if the data controller committed the offense willfully, in exchange for pay-