2015

Data Protection in Clinical Trials: Adapting EU Solutions to US Research

Phillip DeFedele

Phillip DeFedele

DATA PROTECTION IN CLINICAL TRIALS: ADAPTING EU SOLUTIONS TO US RESEARCH

I. Introduction

Clinical trials are the primary basis upon which the U.S. Food and Drug Administration (FDA) determines whether there is substantial evidence to support efficacy claims of new drugs as well as whether such drugs are safe.[1] Clinical trials are studies in which human subjects are administered a new drug and they constitute a substantial part of the entire research and development process and are essential in order to obtain FDA approval of a new drug.[2] Clinical trials take, on average, six to seven years to complete out of a total of ten to fifteen years for research and development.[3] Thousands of patients may be enrolled in clinical trials through all three phases and, consequently, there are many actors involved in the conduct of such studies.[4] Due to the increasing presence of these many different actors involved in such trials, data obtained from those enrolled in the study must be transferred to and from these various actors.[5] These particular transfers of data in the course of a single clinical trial are the subject of this paper.

Data collected from clinical trials are entitled to special legal protections in order to safeguard the confidentiality and privacy of the human subjects involved in such research. In the United States, such protections are set forth in the Common Rule as well as FDA regulations, both of which contain additional safeguards for human subjects involved in research.[6] In the European Union (EU), the colloquially known Data Privacy Directive, which broadly applies to

[1] 21 C.F.R. § 314.126.
[2] *Id*.
[3] PHRMA, 2013 PROFILE BIOPHARMACEUTICAL RESEARCH INDUSTRY 32, 34 (2013).
[4] *Id*.
[5] *See infra* Part II.C.
[6] 45 C.F.R. § 46.101 *et seq*.; *see, e.g*., 21 C.F.R. pt. 50 & 56.

all forms of personal data, provides for the protection of data that result from clinical trials.[7] As the times and technology change so must regulations and, consequently, the U.S. Department of Health and Human Services (HHS) has decided to amend the Common Rule to strengthen, among other things, the protection of data obtained from human subject research.[8]

The HHS is seeking to apply requirements from another piece of U.S. legislation, the Health Insurance Portability and Accountability Act (HIPAA), to the Common Rule in order to provide the standards under which the privacy of research data will be protected.[9] Instead of looking domestically, however, it may benefit the HHS, and ultimately the human subjects protected by the Common Rule, to examine non-U.S. methods of data protection, namely the Data Protection Directive, in crafting its own new protections. Ultimately, when it comes to the protection of research data from human subject research, there must be a balance between the interests of providing notice to and protecting the data of human subjects and ensuring that research may occur unhindered in order to encourage innovation and allow new therapies to reach the market as soon as possible. This policy of balancing such interests underlies this paper and ultimately guides the arguments made herein. Part II of this paper shall provide a brief history of human subject research protections, a brief overview of emerging technologies that may be the impetus for revising data protection policies, and an overview of the ANPRM as well as its relevance to FDA regulations and the actors involved in clinical research. Part III will provide an overview of the HIPAA standards that may be incorporated into the Common Rule and how they will apply to clinical trial research. Part IV will explain the applicable legal

[7] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 287/31) [hereinafter "Data Protection Directive"].
[8] Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators, 76 Fed. Reg. 143, 44515 (proposed July 26 2011) [hereinafter "ANPRM"].
[9] *Id*. at 44526.

framework under the Data Protection Directive as it would apply to clinical trials in the EU. Part V shall compare and contrast HIPAA and the Data Protection Directive with regards to research and advocate that the Data Protection Directive provides the best balance of the aforementioned policy interests. Lastly, Part VI concludes the paper.

II. Evolution of Human Subject Research Protections, Data Protection Concerns in Emerging Technologies, and Regulatory Schemes

A. Evolution of Human Subject Research Protections

Prior to World War II, there was no international statement of ethical principles that should govern human experimentation.[10] Protections for human subjects originated from the Nuremberg Code[11] which resulted from the Doctors' Trial in which Nazi doctors were put on trial for experiments carried out in concentration camps. The Nuremberg Code set forth ten principles pursuant to which research should be conducted.[12] The most influential early document on human subject research protections, however, is the World Medical Association's Ethical Principles for Medical Research Involving Human Subjects[13], more commonly referred to as the Declaration of Helsinki.[14] The Declaration of Helsinki was developed by the World Medical Association (WMA) as "a statement of ethical principles for medical research involving human subjects, including research on identifiable human material and data."[15] The Declaration of Helsinki has been amended since its initial adoption in June of 1964 and contains general principles as well as special attention to, among other things, vulnerable populations, risks and

[10] Delon Human & Sev Fluss, *The World Medical Association's Declaration of Helsinki: Historical and Contemporary Perspectives* 4 (July 24, 2001), http://www.wma.net/en/20activities/10ethics/10helsinki/draft_historical_contemporary_perspectives.pdf.
[11] *The Nuremberg Code*, U.S. Department of Health & Human Services (last visited Oct. 10 2014), http://www.hhs.gov/ohrp/archive/nurcode.html.
[12] *Id*.
[13] Declaration of Helsinki, June 1964.
[14] Human, *supra* note 10, at 2.
[15] Declaration of Helsinki.

benefits, protocols, ethics committees, and informed consent.[16] The Declaration of Helsinki also contains a principle concerning privacy and confidentiality which declares that "[e]very precaution must be taken to protect the privacy of research subjects and the confidentiality of their personal information."[17] Thus, even before the advent of modern technological advances, the privacy of individuals was already a concern on an international level.

In the United States, the National Research Act of 1974 established the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research ("National Commission"), which was tasked with identifying the basic ethical principles that should guide the conduct of research involving human subjects.[18] In doing so, the National Commission produced the Belmont Report which summarizes the basic ethical principles for conducting human subject research.[19] The National Commission set forth three principles in the Belmont Report: (1) respect for persons; (2) beneficence; and (3) justice.[20] The principle of respect for persons encompasses the requirement to acknowledge autonomy and the requirement to protect those with diminished authority.[21] The principle of beneficence is an obligation to do no harm and maximize possible benefits while minimizing possible harms.[22] The final principle of justice is a sense of fairness in distribution and that equals should be treated equally.[23] Most

[16] *Id*.
[17] *Id*.
[18] The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research*, Apr. 18, 1979 [hereinafter "The Belmont Report"].
[19] *Id*.
[20] *Id*.
[21] *Id*.
[22] *Id*.
[23] *Id*.

significantly, the Belmont Report influenced the United States' human subject regulations resulting in both the HHS and the FDA revising their respective human subject regulations.[24]

The preeminent federal regulations regarding human subject research are embodied in the Common Rule which was first published in 1991 by the HHS.[25] The Common Rule applies to all research involving human subjects that is conducted or supported, meaning funded in whole or in part, by a federal department or agency.[26] A human subject is defined as a "living individual about whom an investigator . . . conducting research obtains . . . [d]ata through intervention or interaction with the individual, or . . . [i]dentifiable private information."[27] Under the Common Rule, research is defined broadly as "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge."[28] The Common Rule goes on to explain that an intervention may be a physical procedure by which data are gathered or manipulations of the subject, or his or her environment, performed for research purposes.[29] Moreover, an interaction may be a communication or interpersonal contact between the investigator and subject.[30] Given the collection of data involved in research, the Common Rule also addresses the concept of private information.[31]

Private information under the Common Rule includes information about "behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information which has been provided for specific purpose by an individual

---

[24] *Federal Policy for the Protection of Human Subjects ('Common Rule')*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES (last visited Nov. 17, 2014), http://www.hhs.gov/ohrp/humansubjects/commonrule/.
[25] *Id*.
[26] 45 C.F.R. § 46.101.
[27] 45 C.F.R. § 46.102(f).
[28] 45 C.F.R. § 46.102(d).
[29] *Id*.
[30] *Id*.
[31] *Id*.

and which the individual can reasonably expect will not be made public."[32] Moreover, private information must be individually identifiable, meaning that "the identity of the subject is or may readily be ascertained by the investigator or associated with the information", in order for the ascertainment of such information to be considered research involving human subjects.[33] Despite the attention given to defining private information, the Common Rule simply places the burden on institutional review boards ("IRBs") to be responsible for protecting the privacy of subjects and data.[34] Specifically, an IRB must determine that, among other things, there are "adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data" prior to approving research.[35] Although this provision may have been appropriate when the Common Rule was originally promulgated in 1991, the advent of new technologies resulting in increased informational risks requires more robust protections.[36]

B. Data Protection Concerns in Emerging Technologies

There are increasing uses of genetic information, biospecimens, and databases in research that result in informational risks, meaning risks of inappropriate uses or disclosures of human subjects' information.[37] Wrongful disclosures, such as those relating to substance abuse or chronic illness, may have practical adverse effects on a particular research subject, including jeopardizing employment and causing emotional and social harms.[38] Two types of research techniques that incite such risks are bioinformatics and functional genomics.[39]

---

[32] *Id*.
[33] *Id*.
[34] 45 C.F.R. § 46.111(a)(7).
[35] *Id*.
[36] ANPRM, *supra* note 8, at 44513–44514.
[37] *Id*.
[38] *Id*. at 44516.
[39] YALI FRIEDMAN, BUILDING BIOTECHNOLOGY: BIOTECHNOLOGY BUSINESS, REGULATIONS, PATENTS, LAW, POLICY AND SCIENCE 41, 46 (2014).

Bioinformatics applies information technology to manage and analyze research data, which assists scientists in managing and interpreting such data.[40] Bioinformatics utilizes computers to assist in data management which permits the collection and analysis of biological information, including deoxyribonucleic acid (DNA) sequencing.[41] The advantage of bioinformatics is the ability to extract information and detect certain patterns from large databases.[42] Bioinformatics is also able to analyze masses of information and allow comparative analyses.[43] Clearly, the ability to access and analyze large databases is susceptible to informational risks of improper disclosure or uses.

Functional genomics focuses on gene activity in both healthy and diseased states, which allows analyses of how genetic variations may account for different levels of efficacy of a drug in certain populations.[44] Specifically, pharmacogenetics studies how genetic differences affect how people respond to drugs in order to understand variations between drug targets and enzymes that affect efficacy and toxicity.[45] This technique allows researchers to develop drugs that are capable of addressing the effects genetic variations may have on safety and efficacy.[46] Pharmacogenetics rely upon analyses of individuals' genetic information, which is certainly the most unique and personal information about an individual, and, therefore, must have adequate privacy protections in place.

All in all, these emerging research technologies must be subject to adequate data protections in order to not only ensure that such data is protected, but also to make sure that such

[40] *Id*. at 41–42.
[41] *Id*. at 42.
[42] *Id*. at 43.
[43] *Id*.
[44] *Id*. at 46.
[45] *Id*. at 47.
[46] *Id*. at 48.

data is seen to be protected by regulators and subjects.[47] Although one can argue that stringent protections may hinder research, the fact remains that research depends upon voluntary contribution and, therefore, if subjects were to lose faith in the safeguards in place to protect their data, it would have an adverse effect on their willingness to participate, which would impede new research.[48] Therefore, adequate privacy protections are not only necessary for the protection of human subjects but are also necessary to ensure the continued success of research and the utilization of new research techniques.

C. From the Common Rule to FDA Regulations

As further discussed below, the HHS in its ANPRM seeks to modify, among other things, the protection of data obtained from human subjects in the Common Rule.[49] The Common Rule, however, only applies to research that is either conducted or financially supported by a federal agency.[50] Therefore, absent such agency involvement, the Common Rule does not apply to a vast amount of research undertaken to achieve FDA approval of a new pharmaceutical product since they are typically privately funded by the sponsor.[51] Such studies, however, are governed by FDA regulations codified in Title 21 of the Code of Federal Regulations.[52] Although research using federal funding and those for FDA approval are governed by different regulatory regimes, both sets of regulations stem from the same ethical foundation, specifically the Belmont

[47] MARK TAYLOR, GENETIC DATA AND THE LAW: A CRITICAL PERSPECTIVE ON PRIVACY PROTECTION 5 (Margaret Brazier et al. eds., 2012).
[48] *Id*.
[49] ANPRM, *supra* note 8, at 44513–44514.
[50] 45 C.F.R. § 46.101.
[51] Although it is often the case that pharmaceutical companies entirely fund their own research, an example of an exception to this is when a pharmaceutical company receives funding from the Biomedical Advanced Research and Development Authority (BARDA). *See, generally*, *Biomedical Advanced Research and Development Authority – PHE*, PUBLIC HEALTH EMERGENCY (last visited Nov. 22, 2014), http://www.phe.gov/about/barda/Pages/default.aspx.
[52] *See, e.g.*, 21 C.F.R. 56.101 *et seq*.

Report.[53] Thus, respect for persons, beneficence, and justice, the three ethical principles laid out in the Belmont Report, are equally applicable to both the Common Rule and FDA regulations governing human subject research.

A more concrete example of this connection is the nearly identical language contained in both the Common Rule and FDA regulations.[54] Like under the Common Rule, an IRB overseeing research subject to FDA regulations must ensure, among other things, that there are "adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data" in order to approve the research study.[55] This is the exact same language contained in the Common Rule's section concerning IRB approval of research.[56] Given these strong parallels in origins and language, the considerations involving the reformation of the Common Rule should also apply to FDA regulations. In fact, because the Common Rule is only limited to studies receiving federal funding, there is a more urgent need to amend the FDA regulations given the vast amount of subjects involved and studies.[57] Therefore, the revisions to the Common Rule and recommendations contained herein should apply and encourage equivalent modifications to the FDA regulations.

As discussed further below, these revisions to the Common Rule were partially motivated by the increase in the amount of actors involved in the conduct of clinical trials. For starters, there is the sponsor, which, in most instances, is the pharmaceutical company seeking approval for its new drug.[58] The sponsor initiates and maintains ultimate responsibility for a clinical trial.[59] A sponsor's obligations include, among other things, selecting investigators, monitoring the

---

[53] *See supra* note 24.
[54] *Compare* 45 C.F.R. § 46.111(a)(7) *with* 21 C.F.R. § 56.111(a)(7).
[55] 21 C.F.R. § 56.111(a)(7).
[56] *Compare* 45 C.F.R. § 46.111(a)(7) *with* 21 C.F.R. § 56.111(a)(7).
[57] *See supra* Part I.
[58] 21 C.F.R. § 312.3.
[59] *Id*.

investigations, and ensuring that the study is conducted in accordance with the protocol.[60] The sponsor may, however, delegate its responsibilities regarding the conduct of a study to a contract research organization (CRO).[61] In such an instance, the CRO would be the middle man between the sponsor and any clinical trial sites. Moreover, each site where the clinical trial is taking place has a principal investigator that leads the conduct of the study as well as a study team made up of various personnel.[62] Additionally, depending upon the nature of the clinical trial, the sponsor may utilize a Data Safety Monitoring Board (DSMB) to review the un-blinded data from the clinical trial in order to evaluate the safety of trial subjects and the validity and scientific merit of the trial.[63] Thus, these various actors that, in part, spurred the HHS to revise the Common Rule further demonstrate the vast amounts of data transfers that occur in conducting clinical trials which must be subject to heightened data protection standards.

D. Advanced Notice of Proposed Rulemaking

The HHS released the ANPRM in order to address the drastically changed landscape of research since the Common Rule's enactment in 1991 and to comply with the President's Executive Order requiring federal agencies to review their respective regulations in order to make such regulatory schemes more effective and less burdensome.[64] The HHS explains that, not only have research techniques changed, but also that many actors, in addition to the sponsor and principal investigators, have joined the research enterprise.[65] In the ANPRM, the HHS notes that there are doubts as to whether the current regulatory framework is sufficient for the protection of

[60] 21 C.F.R. § 312.50.
[61] 21 C.F.R. § 312.23.
[62] BAKER & MCKENZIE, CLINICAL TRIALS A GLOBAL HANDBOOK 617 (2010).
[63] FDA, OMB CONTROL NO. 0910-0581, GUIDANCE FOR CLINICAL TRIAL SPONSORS: ESTABLISHMENT AND OPERATION OF CLINICAL TRIAL DATA MONITORING COMMITTEES (2006).
[64] Exec. Order No. 13,563 (2011); ANPRM, *supra* note 8, at 44513.
[65] ANPRM, *supra* note 8, at 44513.

human subjects.[66] The ANPRM seeks to amend the Common Rule to alleviate concerns about its adequacy in protecting human subjects and to respond to criticisms of the Common Rule related, to among other things, IRB review of research, informed consent, and increasing informational risks.[67] As part of this overhaul, the ANPRM seeks to impose HIPAA standards for the protection of data in order to remedy the increased informational risks that are present in human subject research.[68] The ANPRM urges that the current Common Rule approach requiring IRBs to evaluate informational risks may not be the best methods of minimizing such risks due to a potential lack of expertise regarding data protection.[69] The ANPRM proposes to apply mandatory data standards as set forth under HIPAA to apply to all data that are collected, generated, stored, or used in human subject research.[70] Therefore, the ANPRM seeks to enforce standards for the protection of data based on those set forth in HIPAA in all research studies governed by the Common Rule.[71]

III. HIPAA

Congress enacted HIPAA in 1996 in order to, among other things, improve the portability and continuity of health insurance coverage, and to combat waste, fraud and abuse in the health insurance and health care delivery systems.[72] The HHS had the responsibility to promulgate regulations regarding the privacy of individuals' health information.[73] These regulations encompass the HIPAA Privacy Rule, which is meant to assure that individuals' health information is protected while allowing such information to be transmitted in order to promote

[66] *Id*.
[67] *Id*. at 44513–44514.
[68] *Id*.
[69] *Id*. at 44516.
[70] *Id*.
[71] *Id*. at 44526.
[72] Pub. L. 104-191.
[73] U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, SUMMARY OF THE HIPAA PRIVACY RULE 1 (2003).

high quality healthcare.[74] The HIPAA Privacy Rule only applies to "covered entities" which are defined as health plans, healthcare clearing houses, and healthcare providers.[75] A healthcare provider may be a person or entity that provides, bills for, or is paid for healthcare in the normal course of business.[76] Although HIPAA mainly protects medical records and other related data used in providing and reimbursing healthcare and a pharmaceutical manufacturer is not a covered entity, the Privacy Rule already applies to research in a limited manner.[77] Pharmaceutical manufacturers must utilize hospitals and physicians in order to conduct clinical trials.[78] Hospitals and practicing physicians that are not solely involved in the conduct of research fit the statutory definition of a healthcare provider under HIPAA.[79] Therefore, when interacting with patients on an individual site level, the principal investigator, institution, and members of the study team that constitute covered entities are already bound by the provisions of HIPAA. Under the ANPRM, however, the concept of a covered entity is essentially moot because HIPAA privacy standards would apply to all actors involved in the clinical trial that are handling protected health information.[80]

Under HIPAA, covered entities are broadly prohibited from using or disclosing protected health information except when permitted to do so, such as pursuant to a valid authorization.[81] Protected health information (PHI) is defined as "individually identifiable health information" that is transmitted or maintained in any form or medium.[82] Individually identifiable health information is a subset of health information that identifies the individual or with respect to

[74] *Id*.
[75] 45 C.F.R. § 160.103.
[76] *Id*.
[77] *Id*.
[78] *See supra* Part I.
[79] 45 C.F.R. § 160.103.
[80] ANPRM, *supra* note 8, at 45516.
[81] 45 C.F.R. § 164.502(a).
[82] 45 C.F.R. § 160.103.

which there is a reasonable basis to identify the individual from such information.[83] Health information is defined as "any information . . . whether oral or recorded in any form or medium, that: "[among other things,] relates to the past, present, or future physical or mental health or condition of an individual."[84] The concept of PHI also applies to individuals that have been deceased for 50 years or less.[85] Although such data is considered PHI, it may be disclosed and used under HIPAA provided such use or disclosure is solely for research, documentation of the death of the individual is provided, and such use or disclosure is necessary for the research.[86]

In the context of clinical trials, any data obtained from the subjects would constitute "health information" under HIPAA as they would relate to the health or condition of an individual and the drug's effect on his or her health or condition. HIPAA, however, only applies to individually identifiable health information and, therefore, if the information is properly de-identified, it is not subject to HIPAA protections.[87] Thus in the context of clinical research, if a principal investigator were to de-identify any data collected from a research subject, he or she may freely transmit it to any entity, such as the sponsor or CRO.

It is no easy task to de-identify data, however. There are two methods by which data can be de-identified.[88] First, an expert with expertise in statistical and scientific principles and methods for identification may de-identify the data by applying such principles and methods and subsequently determine that the risk for re-identification is very small.[89] Second, specific identifiers must be removed from the data related to, not only the individual, but also any

[83] 45 C.F.R. § 160.103.
[84] 45 C.F.R. § 160.103 (2013).
[85] *Id*.
[86] 45 C.F.R. § 164.512(i)(1)(iii).
[87] 45 C.F.R. § 164.502.
[88] 45 C.F.R. § 164.514(b).
[89] 45 C.F.R. § 164.514(b)(1).

relatives, employers, or household members of the individual.[90] The identifies are names, geographic subdivisions smaller than a state, all elements of dates except year (in most instances), telephone and fax numbers, e-mail addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate and license numbers, vehicle identifiers and serial numbers, device identifiers and serial numbers, URLs, IP addresses, biometric identifiers, full face images, and any other unique identifiers.[91] In order to qualify as de-identified information under these two methods, the procedures set forth therein must be strictly followed. Even limited data sets, which are discussed below, that have almost all identifiers removed are still considered PHI and subject to the protections of HIPAA.[92]

Given the complexities of de-identifying data, there are two main methods by which data could be transferred from one entity to another without having to be completely de-identified. The first is through an authorization from the human subject and the second is through the use of limited data sets.[93] HIPAA clearly states that an entity may not use or disclose PHI without a valid authorization, except as otherwise provided.[94] There are specific standards that an authorization must meet in order to be considered valid.[95] First, there are certain core elements that an authorization must fulfil which are a description of the information to be used in a specific manner, the name of the person/entity authorized to make the disclosure, the name of the person/entity to whom such information will be disclosed, a description of the purpose of such disclosure, an expiration date or event upon which the authorization will expire, and the signature of the individual and date.[96] It is permissible for an authorization to not have an

[90] 45 C.F.R. § 164.514(b)(2).
[91] *Id*.
[92] 45 C.F.R. § 154.514(e)(2).
[93] 45 C.F.R. §§ 164.508(a) & 164.514(d)(5)(e)(1).
[94] 45 C.F.R. § 164.508(a).
[95] 45 C.F.R. § 164.508(c).
[96] 45 C.F.R. § 164.508(c)(1).

expiration date when used for research purposes, including the establishment and maintenance of research databases.[97] In addition to these core requirements, an authorization must also make certain statements that provide adequate notice to the individual of his or her right to revoke the authorization in writing and any limitations thereon and the ability or inability to condition, among other things, treatment on whether the individual signs the authorization.[98] Regarding the revocation of an authorization, an individual is permitted by HIPAA to revoke a valid authorization at any time in writing unless the authorized entity has acted in reliance thereon.[99] Lastly, an authorization must be written in plain language understandable by the research subject.[100]

In addition to the standard authorization provisions described above, authorizations for research purposes are able to be used for future research and combined with other forms, such as the informed consent form for the study. As expressed by the HHS in the publication of the final HIPAA Omnibus Rule, authorizations may be used for future research studies.[101] An authorization for future research purposes is valid so long as such future purposes are adequately described so that "it would be reasonable for the individual to expect that his or her PHI could be used or disclosed for such future research."[102] Although the HHS acknowledges that such purposes could include specific statements, it does not require them.[103] It is important to note that this does not require the subject to have actual knowledge of such other studies. In addition to authorizing future research, research authorizations may be compounded with other documents

[97] 45 C.F.R. § 164.508(c)(1)(v).
[98] 45 C.F.R. § 164.508(c)(2)(i)–(ii).
[99] 45 C.F.R. § 164.508(b)(5)(i).
[100] 45 C.F.R. § 164.508(c)(3).
[101] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 17, 5612 (Jan. 25, 2013).
[102] *Id*.
[103] *Id*.

in order to create a compound authorization.[104] Specifically, an authorization for research may be combined with any other written permission regarding that particular study or another study.[105] This includes combining an authorization with an authorization for the creation and maintenance of research databases or with the informed consent form to participate in the research.[106] Although HIPAA authorizations are a straightforward and transparent means by which a human subject's data may be transferred from one actor in the clinical trial to another, there is another means by which such data could be transferred without requiring the subject's consent.

An entity may also use what HIPAA calls "limited data sets" to disclose data to a third party without obtaining authorization from the data subject provided that the entity and the third party enter into a data use agreement.[107] Limited data sets must be de-identified in a similar manner to completely de-identified information although with less requirements.[108] Similar to complete de-identification, a limited data set must exclude certain direct identifiers of the individual or of any relatives, employers, or household members of such individual.[109] The identifiers are names, postal/street addresses, telephone and fax numbers, e-mail addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate and license numbers, vehicle identifiers and serial numbers, device identifiers and serial numbers, URLs, IP addresses, biometric identifiers, and full face images.[110] As noted, this de-identification process differs from complete de-identification only in that limited data sets may contain dates, political subdivisions smaller than a state, and do not broadly

[104] 45 C.F.R. § 164.508(b)(3)(i).
[105] *Id*.
[106] *Id*.
[107] 45 C.F.R. § 164.514(d)(5)(e)(1).
[108] *Compare* 45 C.F.R. § 164.514(d)(5)(e)(2) *with* 45 C.F.R. § 164.514(b)(2).
[109] 45 C.F.R. § 164.514(d)(5)(e)(2).
[110] *Id*.

prohibit other unique identifiers.[111] Limited data sets are only permitted to be used in a limited number of circumstances, namely, for purposes of research, public health, or healthcare operations.[112]

In order to disclose limited data sets without needing to obtain the individual's authorization, the disclosing entity must enter into a data use agreement with the recipient of such information.[113] The data use agreement is meant to obtain assurance that the recipient will only use or disclose the data set for limited purposes.[114] As with authorizations, however, data use agreements must meet specific requirements.[115] A data use agreement must establish the permitted uses and disclosures of the data set, set forth who is permitted to receive or use the data set, and provide that the recipient will use and disclose the data only in accordance with the agreement, use appropriate safeguards to prevent unauthorized uses or disclosures of the data set, report to the disclosing entity any inappropriate uses or disclosures, ensure that any agents to whom it provides such data agree to the same terms and conditions of the data use agreement, and not identify or contact the individual.[116]

In terms of research, a HIPAA authorization allows data to be transferred to another entity without the need to significantly de-identify the information and enter into agreements with such entities. Moreover, an authorization has several benefits in the context of research, such as being able to be combined with the informed consent form and authorizing future research. An authorization also more adequately balances the interests of notice and protection of human subjects and uninhibited research, especially considering that limited data sets do not

[111] *See supra* note 90.
[112] 45 C.F.R. § 164.514(d)(5)(e)(3)(i).
[113] 45 C.F.R. § 164.514(d)(5)(e)(4)(i).
[114] *Id*.
[115] 45 C.F.R. § 164.514(d)(5)(e)(4)(ii).
[116] *Id*.

require notice to the subject. Importantly, a subject also has the opportunity to revoke an authorization. Therefore, the HIPAA authorization will be the basis for comparison against the EU legal framework for transferring data from one actor to another.

IV. EU Data Protection

The EU has taken a very different approach to data protection from the United States and, in fact, has explicitly established a right to data protection, which is considered a fundamental right.[117] The EU adopted Directive 95/46/EC[118] (the "Data Protection Directive" or the "Directive"), more commonly known as the Data Protection Directive, in order to ensure that "the level of protection of the rights and freedoms of individuals with regard to the processing of personal data is equivalent in all Member States."[119] Unlike HIPAA, the Data Protection Directive applies to all forms of "personal data" as defined in the directive.[120] The Data Protection Directive applies to all 28 EU Member States[121] as well as non-EU Member States[122] that are part of the European Economic Area (EEA).[123] It is important to note that the Data Protection Directive acts as a framework which each individual Member State's national laws regarding data protection must follow.[124] To parallel the U.S. regulatory scheme, the Directive could be seen as the enabling statute which dictates the mission of an agency and purpose for which it may promulgate regulations; whereas, the national laws would be the regulations

---

[117] COUNCIL OF EUROPE ET AL., HANDBOOK ON EUROPEAN DATA PROTECTION LAW 20 (2014) [hereinafter "Handbook"].
[118] Directive, *supra* note 7.
[119] Handbook, *supra* note 117, at 18.
[120] Directive, *supra* note 7, at art. 1.
[121] The 28 EU Member States are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom.
[122] The non-EU Member States are Iceland, Liechtenstein, and Norway.
[123] Handbook, *supra* note 117, at 18.
[124] *Id*.

implementing the statute. This paper will focus on the basic mechanism under the Directive that permits the transfer of personal data from one actor in a clinical trial to another.[125]

The Data Protection Directive relies heavily on concepts of "personal data", "processing of personal data", and consent in order to function. The Data Protection Directive makes a blanket prohibition on the processing of personal data unless, among other legitimate legal bases, the data subject has unambiguously given his or her consent.[126] Moreover, not all personal data is treated equally under the Data Protection Directive as there are additional protections for special categories of personal data.[127] Even for these special categories, however, consent is a valid basis for processing such data provided it is made explicitly.[128]

"Personal data" is defined as "any information relating to an identified or identifiable natural person."[129] Such identified or identifiable persons are referred to as "data subjects."[130] An identifiable person means that such person can be identified, directly or indirectly, which means, in practice, that additional information capable of identifying the person can be acquired without unreasonable effort.[131] It is important to note that the Data Protection Directive only refers to natural persons and, therefore, only natural persons are covered by its protections.[132] Moreover, its protections only apply to living persons.[133] As previously mentioned, there are special categories of personal data, known as "sensitive data", which are subject to heightened protections.[134] Sensitive data include, among other things, data concerning health or racial or

[125] In reality, the Data Protection Directive is a complex piece of legislation that is not as simple as explained in this paper. As mentioned, this paper has a limited focus on the basic requirements for processing personal data.
[126] Data Protection Directive, *supra* note 7, at art. 7(a).
[127] *Id.* at art. 8.
[128] *Id.*
[129] *Id.* at art. 2(a).
[130] *Id.*
[131] *Id.*; Handbook, *supra* note 117, at 36.
[132] Handbook, *supra* note 117, at 37–38.
[133] *Id.* at 37.
[134] Data Protection Directive, *supra* note 7, at art. 8; Handbook, *supra* note 117, at 36.

ethnic origin.[135] In the context of clinical trials, the data gathered from the subjects regarding their medical condition and the effects of the subject drug on such condition as well as any genetic data collected constitute sensitive data and are subject to the heightened legal regime for processing such data.

"Processing of personal data" means "any operation or set of operations which is performed upon personal data, whether or not by automatic means."[136] Such means include, but are not limited to, collection, recording, storage, use, disclosure by transmission, dissemination, erasure, and destruction.[137] It is clear that the concept of data processing is incredibly broad and covers a wide variety of activities even those as simple as talking.[138] The aspect of processing of personal data examined in the context of this paper is the transfer of personal data from one actor to another in the setting of clinical trials. As already discussed, personal data may not be processed absent a legitimate legal basis such as consent. The concept of consent; however, is more than simply signing off on a request to process data as seen with HIPAA authorizations.

The Directive defines consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[139] In order to be valid, however, the consent must fulfill the following elements: (1) the data subject must have been under no pressure to consent; (2) the data subject must have been informed of the object and consequences of consenting; and (3) the scope of consent must be reasonably concrete.[140] Regarding the second element, the data subject must have sufficient information to make his or her decision, as determined on a case-by-case basis, in the form of a

---

[135] *Id*.
[136] Data Protection Directive, *supra* note 7, at art. 2(b).
[137] *Id*.
[138] In fact, the Data Protection Directive explicitly exempted the processing of personal data by a natural person for purely personal or household purposes. Data Protection Directive, *supra* note 7, at art. 3(2); Handbook, *supra* note 117, at 19.
[139] Data Protection Directive, *supra* note 7, at art. 2(h).
[140] Handbook, *supra* note 117, at 56.

precise and easily understandable description of the subject matter, including the consequences of consenting or the refusal to do so.[141] The third element requires that the consent be specific as determined by the "reasonable expectations of an average data subject."[142] If the processing operations are to be changed or additional operations added in a way that could not reasonably have been seen at the time of initial consent, the data subject's consent must be obtained again.[143] Provided the consent process fulfills these three elements and is made explicitly, a data subject, such as a human research subject, may have his or her sensitive data processed lawfully.[144] There is a general recognition of a data subject's right to withdraw consent that he or she can exercise at any time and at his or her discretion.[145] Moreover, a data subject is not required to give any reason for the withdrawal and cannot be subject to adverse consequences as a result of such withdrawal.[146] There is a unique nuance to the withdrawal of consent, however. The withdrawal of consent only applies to data processing to occur in the future, not that which has already occurred.[147] If there is no legal basis to justify the further storage of such data after the withdrawal of consent, however, the data should then be deleted wherever such data is stored.[148] Therefore, although the data subject consented to the initial collection of data, the storage of such data is no longer permissible once consent is withdrawn and there is no additional legal basis for further processing.

As a corollary to the consent process, personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those

---

[141] *Id*. at 59.
[142] *Id*.
[143] *Id*. The Directive does, however, provide a limited exception to this rule if the data is further processed for historical, statistical, or scientific purposes, provided there are appropriate safeguards. Data Protection Directive, *supra* note 7, at art. 6(1)(b).
[144] Data Protection Directive, *supra* note 7, at art. 8(2)(a).
[145] Handbook, *supra* note 117, at 60.
[146] *Id*.
[147] ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 15/2011 ON THE DEFINITION OF CONSENT 33 (2011).
[148] *Id*.

purposes."[149] The entity that is processing the data must specify the purpose of the processing and notify the data subject of such purpose prior to the processing of his or her data.[150] Echoing the requirement that consent be specific, it is unlawful to process data for undefined or unlimited purposes.[151] For every new purpose, there must be a particular legal basis in order to process the data for such purpose.[152] Yet, if a new purpose is not incompatible with the initial purpose, the data subject's original consent may be a sufficient basis for the new purpose.[153] In assessing compatibility there are four key factors that must be considered: (1) "the relationship between the purposes for which the data have been collected and the purposes of further processing"; (2) "the context in which the data have been collected and the reasonable expectations of the data subjects as to their further use"; (3) "the nature of the data and the impact of further processing on the data subjects"; and (4) "the safeguards applied . . . to ensure fair processing and to prevent any undue impact on the data subjects."[154] As an initial matter, this assessment should be carried out by the entity processing data; however, in the event of litigation, the court would then undertake this analysis.[155]

The first factor focuses on the substance of the relationship between the original purpose and the purpose of further processing.[156] The relationship may cover situations where the further processing was implied in the original purpose or situations where there is a partial or non-existent link with the original purpose.[157] The greater the differences between the purposes, the

[149] Data Protection Directive, *supra* note 7, at art. 6(1)(b).
[150] Handbook, *supra* note 117, at 68.
[151] *Id*.
[152] *Id*.
[153] *Id*. at 69.
[154] ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 03/2013 ON PURPOSE LIMITATION 23–26 (2013).
[155] *Id*. at 14.
[156] *Id*. at 23.
[157] *Id*. at 24.

more problematic it is for establishing compatibility.[158] The second factor involves the issue of "what a reasonable person in the data subject's situation would expect his or her data to be used for based on the context of the collection."[159] Generally, the more unexpected or surprising the further use is, the more it will be considered to be incompatible.[160] If the original collection of the information was restrictive and specific, it is likely that there will be more limitations on further use.[161] Importantly, the relationship between the data subject and individual or entity processing the data must be taken into account to determine whether there were inequalities in bargaining power or coerciveness during the informed consent process.[162] If so, this factor will weight against finding that the additional purpose is compatible with the original one.[163]

The third factor requires analysis of whether the further processing involves sensitive data which require special protections.[164] If the information is sensitive, including medical and genetic data, the scope for compatible uses is narrow.[165] Additionally, both positive and negative consequences must be considered in determining the impact of further processing.[166] This inquiry also includes an analysis of the way in which the data are further processed such as processing by a third party and public disclosure or disclosure to a wide range of persons, especially if unforeseeable at the time of data collection.[167]

The final factor looks at the safeguards which are in place and may serve as a counterbalance to any factors that weigh in favor of a finding of incompatibility.[168] The Working

[158] *Id*.
[159] *Id*.
[160] *Id*.
[161] *Id*.
[162] *Id*.
[163] *Id*.
[164] *Id*. at 25.
[165] *Id*.
[166] *Id*.
[167] *Id*.
[168] *Id*. at 26.

Party has suggested, however, that the first necessary step in ensuring compatibility is to re-specify the purposes by providing additional notice to the data subjects and possibly allowing for them to opt in or out.[169] In some instances obtaining additional consent may be required.[170] All in all, these factors are to be applied on a case-by-case basis and, therefore, there are no bright light rules when it comes to determining compatibility.[171] Because of this fact-sensitive inquiry, it may always be beneficial for one who is processing the data to keep the data subject informed in order to ensure that they are on notice and have the ability to consent to any further processing. This can easily be accomplished in clinical trials where researchers often follow up with subjects after the administration of a new drug. Therefore, if the subject's data needs to be transferred for another purpose not contemplated in his or her original consent, it is possible to notify the subject of such purpose and obtain consent.

As discussed, the Data Protection Directive allows personal data to be transferred from one actor in a clinical trial to another by obtaining the subject's informed consent which elevates function over form and is an organic process encouraging constant communication between the researcher and subject. Additionally, the purpose of the transfer must be concrete and cannot be unlimited or undefined. Most significantly, a subject has the absolute right to revoke his or her consent which requires the deletion of his or her personal data absent an additional legal basis for the continued use or storage thereof. These key aspects of the Directive will be compared to HIPAA.

V. Similar Processes with Significant Differences

As a practical matter, HIPAA and the Data Protection Directive are relatively similar regarding the ease of transferring data from one entity to another. Both regimes allow for the

[169] *Id*.
[170] *Id*.
[171] *Id*. at 21.

collection of a research subject's permission to use and transfer his or her data to another party at the initial time of contact, such as the informed consent process for participating in the trial. HIPAA does this through obtaining a written and signed authorization; whereas, the Directive achieves this through its own informed consent process.[172] Additionally, regardless of the process, the research subject must be made aware of the purpose for which the data will be used and who will use such data.[173] Moreover, there are instances in which the research subject's consent may not be required in order to use the data, such as data sets and future research authorizations for HIPAA and compatible purposes and certain secondary uses for the Directive.[174] There are, however, three significant differences between the regimes that, although subtle in some regards, demonstrate that the Directive provides the best balance of protecting the data of and notifying research subjects while unhampering research.

The first major difference is the informed consent process inherent in the Data Protective Directive that is lacking in HIPAA. The Directive requires informed consent in order for data to be collected, processed, and transferred between entities.[175] The consent process, similar to informed consent for medical treatment, is reminiscent of an open dialogue between the data subject and entity or individual obtaining and using such data.[176] The data subject must give the consent willingly and be made aware of the consequences of consenting and the concrete purpose therefor.[177] This is in stark contrast to HIPAA's requirement of an authorization. Although a HIPAA authorization must detail the purpose and who will use the data, HIPAA merely sets forth the requirements that must be contained in an authorization and not which

[172] *See supra* notes 94 & 139.
[173] *See supra* Part III & IV.
[174] *Id*.
[175] *See supra* Part IV.
[176] *Id*.
[177] *Id*.

information should actually be communicated to the research subject.[178] This is a significant distinction between the two legal regimes. Provided that an authorization form contains the necessary elements, the requirements in HIPAA are satisfied; whereas, in order for the requirements of the Directive to be fulfilled, mere documentation is not sufficient as there must be a kind of dialogue between the data subject and researcher.[179] Given the increased informational risks today, ensuring that the research subject has a thorough understanding of the use of his or her data, especially genetic data, is important. Moreover, this requirement further ensures that researchers and those obtaining such data are adequately informing subjects.

Although this requirement may seem stringent and time-consuming, it best balances the interest of providing notice to the subject and allowing research to occur unhindered. For example, in the informed consent process, the data subject may be made aware of the purpose of the collection of his or her data and the processing thereof as well as which entities will be using the data.[180] Therefore, where multiple actors are involved such as CROs, principal investigators, and the sponsor, the connections between them can be made clear and, therefore, the data subject may consent to the processing carried out by such entities.

The informed consent process's advantages do not end there, however. Because the process can be viewed as an ongoing dialogue, it has the possibility to permit other purposes for processing data after initial consent has been obtained that would otherwise be incompatible and, thus, impermissible. As already discussed, a mitigating factor in determining whether an additional purpose is incompatible with the original purpose is notifying the data subject and, if

[178] *See supra* Part III.
[179] *Compare* Part III *with* Part IV. In order to witness the similarities between the Data Protection Directive's informed consent requirements and those for medical treatment *see* FDA, INFORMED CONSENT INFORMATION SHEET: GUIDANCE FOR IRBS, CLINICAL INVESTIGATORS, AND SPONSORS (DRAFT GUIDANCE) (2014).
[180] *See supra* Part IV.

necessary, obtaining further consent.[181] Provided the data subject is able to be contacted, this is only a slight inconvenience in comparison to the protections and notifications it provides.

The second major difference is the Directive's limitations on the amount and types of purposes for processing permissible under a single legal basis while HIPAA has the ability to provide for future authorizations. Although it is a great step in the direction of streamlining and simplifying processes involved in conducting research, HIPAA's allowance of such future authorizations does not truly provide research subjects with proper notice. Under HIPAA, the research subject must be provided adequate notice, which need not contain any specific details, so that the subject could reasonably foresee that his or her information could be used for further research purposes.[182] This is a very low burden to meet. So long as it is reasonably foreseeable that a person's data may be used for future research, which does not rely upon the subject's actual knowledge thereof, the authorization is valid. In reality, this means that a research subject may have no idea in which studies their data are being used and would permit an unlimited amount of uses and studies for which their data are used. While this surely helps encourage research and simplifies the process for making research using such data possible, it completely ignores the principle of providing notice to the research subject. Additionally, because the research subject would not know the definite uses of his or her data, it would cause complications with his or her ability to revoke the authorization. This is so because a research subject may not have approved of a particular study or use of his or her data but, due to a lack of actual knowledge of such study or use, they cannot revoke the authorization for future research.

This is a drastic difference between HIPAA and the Directive. Although the third element of the informed consent process, which requires the scope of consent to be reasonably concrete,

[181] *See supra* note 168.
[182] *See supra* Part III.

is judged by a similar standard of what the reasonable expectations of the average data subject would be, it is compounded and strengthened by the requirement that purposes be specific and concrete.[183] Additionally, under this requirement, there is a blanket prohibition of processing data for undefined or unlimited purposes.[184] Under this blanket rule, it is likely that an authorization for future research under HIPAA would not survive such scrutiny. The true test, however, is whether or not the additional purpose is compatible with the initial purpose of data collection.

As already discussed, this is a fact-sensitive inquiry and there is no readily available answer as to which further research purposes would be permissible and those that would not.[185] In the context of this paper, however, the focus is on clinical trials for drug approval and, therefore, the purposes contained in the informed consent process would be tailored to the particular clinical trial. Therefore, it is unlikely that future studies that are separate and apart from the initial trial in which the subject participates would constitute compatible purposes, especially considering the sensitive nature of the information. Even, for argument's sake, if a particular future purpose would be permissible under HIPAA and the Directive, the aspect of the Directive that sets it above HIPAA in regards to this issue is that, of the factors to be considered in evaluating compatible purposes, the fourth factor, which looks at safeguards in place, helps to mitigate any adverse consequences of the further processing by encouraging the provision of notice to the data subject and/or additional safeguards.[186] Thus, under the Directive, even if consent is not required, there is a high likelihood that notice will be provided to the data subject, so he or she can revoke consent in the event he or she disagrees with such purpose. Moreover, in

[183] *See supra* Part IV.
[184] *See supra* note 151.
[185] *See supra* Part IV.
[186] *See supra* note 168.

the event the data subject cannot be reached due to death, the Directive no longer applies so research will not be inhibited as a result of an occurrence out of the researchers' hands, which is similar to the exception provided in HIPAA.[187] Therefore, once again, in regards to permitting future research/processing, the Directive provides the best balance of providing notice and protection to the data subject while allowing research to continue.

The third major difference is that the right to revoke is treated differently by the Directive and HIPAA. The right to revoke is incredibly important in regards to data protection because it allows the subject to ultimately have the final say in the use of his or her data. Thus, although revocation of consent/authorization makes up a small part of both pieces of legislation, its importance cannot be understated. As such, the distinctions between these legislative acts are incredibly significant in evaluating the superiority of one over the other. The Data Protection Directive, unlike HIPAA, provides an absolute right to revoke consent for data processing.[188] Although HIPAA does provide that a subject may revoke an authorization in writing, it permits limitations to be set thereon as well as restricts this right if such authorization has been relied upon.[189] The Directive, on the other hand, contains an absolute right to revoke which is accompanied by an obligation upon the entity processing the data to delete any collected data.[190] Because the data must be deleted if there is no further legal basis to retain the data, the data subject is able to ensure that no further processing takes place by revoking his or her consent.

It is important to note that HIPAA protects against uses and disclosures of PHI and, therefore, if an authorization is revoked it does not necessarily obligate the formerly authorized entity to delete records of such data. Therefore, adequate protections must still be in place to

[187] *Compare* note 86 *with* note 133.
[188] *See supra* Part IV.
[189] *See supra* Part III.
[190] *See supra* Part IV.

ensure that such data is protected, which have the possibility of failing. The Directive, through its implicit obligation on processors to delete data, however, provides the ultimate safeguard against unlawful processing or disclosure. Additionally, on a personal level, it may give a data subject a sense of relief knowing that his or her data is not just sitting stagnant in a database where there is a real possibility of a data breach. All in all, the right to revoke embedded in the Directive is a powerful tool to ensure that personal data is protected and processed for limited means. This right of revocation, on its own, is substantial evidence of the better suited nature of the Directive to handle sensitive information involved in clinical trials, especially genetic data.

The Directive through its informed consent process, limitations on purposes for which data may be processed under a single legal basis, and right to revoke helps ensure that the interests of notifying data subjects and protecting their data is equally balanced with the interest of carrying out research unhindered. It is this equilibrium that makes the Directive a preferential standard to HIPAA. Although HIPAA, in several respects, falls more on the side of encouraging research, it does not adequately balance this beneficial effect with notification to individuals. Additionally, the inherent limitations on the ability of an individual to revoke an authorization under HIPAA are substantial disadvantages to employing this legal framework. All in all, the Directive is the more appropriate approach to govern the protection of data in the context of clinical trials.

VI. Conclusion

It is clear that the current landscape of clinical trials is complex, and regulators must account for both the safety and integrity of human subjects as well as encouraging innovation. While these interests may seem to conflict, ultimately, ensuring that research subjects are protected allows for their continued voluntary participation in research. Data protection is

increasingly important in this modern age given new research technologies and the types of personal information stored and used for research purposes. The HHS is correct in seeking to revise the Common Rule at this time, but, more importantly, the FDA must follow suit in order to ensure that the majority of research subjects involved in clinical trials for drug approvals can benefit from increased data protections. The HHS's proposal to rely upon mandatory HIPAA privacy standards is admirable and a step in the right direction; however, as discussed, the EU Data Protection Directive more adequately balances the relevant policy interests while protecting human subjects' data. Therefore, the HHS should look to this legal framework when it ultimately decides to enact its reforms in order to ensure that human subjects are adequately protected from information risks while allowing research to continue unhindered due to subjects' willingness to participate in new clinical trials because of such protections.