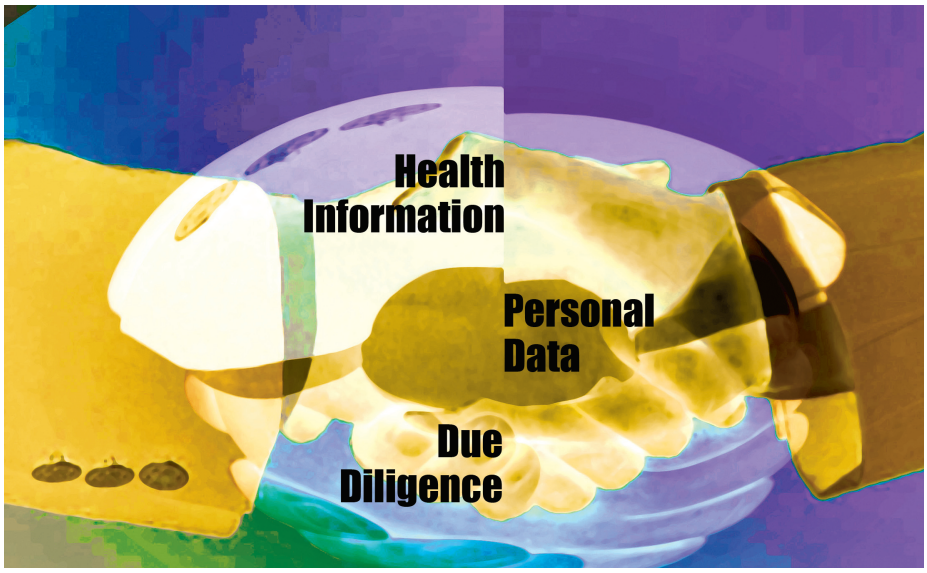
How discreet is your data?

In the final article of this series on sponsors' considerations when negotiating clinical trial contracts with third parties, **Katherine Leibowitz** and **Wim Nauwelaerts** advise on how to protect volunteers' health information and other personal data, and the need to conduct due diligence

KEYWORDS: Clinical trial agreements; HIPAA authorisation; Personal data; Data controller



In order to avoid unnecessary delays in negotiation of the clinical trial contract, as well as unwelcome surprises during the study, the sponsor and other parties involved should carefully consider the respective business needs of all parties to the agreement. It is important to establish from the start a clear understanding and expression of each party's rights and obligations. This article examines the protection of health information and other personal data, and then touches on due diligence procedures.

Protection of personal data: the US

The clinical trial agreement should require the principal investigator (PI) to obtain prior written authorisation to use and disclose health information for research, in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and any applicable US state privacy laws (HIPAA authorisation). The PI should also be required to inform the sponsor of any failure to obtain a HIPAA authorisation before a research subject enrols in the trial. Alternatively, the PI can obtain an appropriate waiver of the authorisation requirement by the institutional review board (IRB) or by a properly constituted privacy board.

Many sponsors propose a form of HIPAA authorisation, but institutions increasingly insist on using their own forms. Institutions' HIPAA authorisations address the needs of the institution and PI, but often fail to address the sponsor's interests sufficiently. Sponsors want to ensure they have access to the trial data at the individual subject level, which would not be possible without a properly drafted HIPAA authorisation. Furthermore, sponsors will be aiming to establish that the breadth of allowable disclosure under the HIPAA authorisation permits them to do what they need or want to do with the trial data.

Regardless of whose HIPAA authorisation form the parties adopt, the sponsor should carefully vet the HIPAA authorisation with HIPAA counsel. In addition, the clinical trial agreement should prohibit the institution and the PI from changing the HIPAA authorisation without the sponsor's consent.

Why is it necessary to include HIPAA language if the agreement contains a general obligation for the parties to comply with applicable laws? From the sponsor's perspective, including appropriate HIPAA language in the clinical trial agreement helps to ensure that data generated by the trial is not marred by a HIPAA violation committed by the institution or the PI. Although the US FDA has not issued a formal statement indicating that it would reject trial data obtained in violation of HIPAA, if such data were in fact obtained in violation of HIPAA then the sponsor would be in a much better position if it could show that it made good-faith efforts, as evidenced by the clinical trial agreement, to require the institution and PI to comply with HIPAA.

The HIPAA language also helps to ensure the sponsor and/or the sponsor's monitors may inspect the research subject records and other source data maintained by the institution. The trial data is the culmination of a vast investment of time and money by the sponsor in its medicine, so every effort should be made to protect the integrity of the trial data and ensure that no legal barriers interrupt the flow of the data.

Protection of personal data: the EU

As far as research subjects' data privacy rights are concerned, the EU clinical trials directive does not impose specific obligations on sponsors or investigators conducting clinical trials in the EU. The directive merely refers to EU Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data (Data Privacy Directive), which has been transposed into the national laws of all EU member states.

Sponsors of clinical trials that involve research subjects in the EU should ensure their trials are conducted in compliance with the data privacy rules of the relevant EU countries. Sponsors can include provisions in their clinical trial agreements to aid them in their compliance effort. However, the data privacy regimes in the different EU countries are not fully harmonised, and some important discrepancies remain, complicating sponsors' compliance efforts.

Types of data. The member states' data privacy legislation covers processing of personal data relating to trial subjects and grants additional protections to 'sensitive' data. The term 'personal data' is defined broadly as any information relating to an identified or iden-

tifiable natural person. In this context, 'processing' means any operation performed on personal data, such as collection, storage, consultation and disclosure, whether or not by electronic means. The term 'sensitive' refers to special categories of personal data – including medical or health-related information – the processing of which is prohibited in principle. Sensitive data can be processed only in exceptional circumstances (for instance, with the research subject's explicit consent) and in accordance with applicable data privacy rules.

In most clinical trials, sponsors will receive case report forms that have been encoded by their investigators, so that sponsors cannot identify individual research subjects. The 'key' to unlock the personal data typically remains with the investigators, who are bound by confidentiality obligations under the clinical trial agreement, as well as by ethics rules. Some EU member states, such as the UK, have taken the position that key-coded data – also often referred to as 'pseudonymised data' – fall outside the scope of data privacy law. In other EU countries, such as France, encoded data constitute personal data as long as someone (for example the sponsor, investigator, or a third person) holds the key to unlock the personally identifiable information hidden in the encoded data. In light of the variation among member states, sponsors should always verify whether the regulators of the relevant EU countries consider encoded trial data as being personal data.

Sponsor obligations. Most member states require the 'data controller' – the person who determines the purposes and the means of processing of personal data – to notify the local data protection authority of the anticipated processing of personal data. The sponsor of a clinical trial is typically considered a data controller for data privacy purposes and would therefore have to notify the relevant data privacy authorities. In most cases, the sponsor will be responsible for filing an information sheet with the competent data privacy authority, specifying among other things the purposes of the data processing, the identity of the recipients of the data and security measures in place to safeguard the data, as well as possible transfers of the data outside the EU.

In exceptional cases, the sponsor may not be the (sole) data controller under applicable data privacy law, and it is therefore advisable to clearly stipulate in the sponsor's clinical trial agreement who will assume the role of data controller and ensure compliance with any filing requirements.

Sponsors should be aware that for sensitive data, some EU member states require a formal opinion, authorisation or permit to be issued by the competent data privacy authority before the data can be processed. In Italy, for example, a sponsor that intends to process health-related data must obtain prior approval from the local data privacy authority, which could take up to 45 days. In Belgium, a simple notification to the Belgian Privacy Commission would suffice and the sponsor would usually be able to start processing the data shortly thereafter.

It is important for sponsors to consider these divergent requirements – which have resulted in a complex web of national filing systems throughout the EU – when setting up a timeframe for their clinical trial. Failure to comply with the obligation to notify or obtain prior authorisation may lead to fines imposed by data privacy authorities or privacy lawsuits, as well as damage to the reputation of the sponsor's business. It should be noted that if the sponsor does not have a physical presence in the relevant member state(s), it could instruct the investigator, institution or CRO to act as its local representative and to register or apply for an authorisation with the relevant data privacy authority.

Sponsors that are viewed as data controllers will also be responsible for implementing adequate security measures to protect research subjects' personal data. The clinical trial agreement should address any security issues and impose appropriate data security obligations on the investigator and/or institution to meet member state requirements.

Informed consent. As in the US, the clinical trial agreement should require the investigator(s) to obtain research subjects' prior written consent with regard to processing of their personal data, taking into account specific restrictions under EU data privacy laws. Although the Data Privacy Directive requires such consent to be explicit, there is no uniform approach across the different member states as to the criteria for a valid consent or the form of such consent. In the Netherlands, for example, the validity of a trial-specific informed consent form could be challenged if the research subject's right to review its personal data is not explicitly stipulated. Therefore, informed consent forms used in one EU country should not be applied in other member states without confirming that the forms comply with applicable data privacy standards.

If the research subjects' consent is used to transfer personal data to jurisdictions outside the EU which do not offer an 'adequate level of data protection' (such as the US), this should be explained in the informed consent form. For example, US companies that are sponsoring trials in the EU and that intend to transfer research subjects' personal data to the US should decide whether they will rely on the research subjects' prior consent as the legal basis for such transfer, or use something else. If the issue of personal data transfer is not properly addressed in the informed consent form, research subjects could dispute the validity of their consent and/or the transfer of their personal data.

It is vital that those sponsors deemed to be data controllers for EU data privacy purposes should review and approve informed consent forms for each EU country individually, since inadequate or poorly drafted informed consent forms could compromise their liability under data privacy laws and ultimately jeopardise the success of the trial.

Due diligence and warranties

As with all business ventures, the sponsor should perform due diligence on its clinical trial business partners before entering into the clinical trial agreement. In addition to standard inquiries regarding medical expertise, patient population, trial facilities and the institution's financial soundness, the sponsor should question whether the hospital, its IRB or ethics committee (EC), and the PI have the sophistication and resources to comply with applicable regulations. For example, a physician widely regarded as an expert in the field may nevertheless not possess comprehensive knowledge of FDA regulations, or may have been cited for regulatory violations in the past.

The sponsor should undertake much of the due diligence before entering into negotiations for the clinical trial, for instance by checking the Warning Letters and Responses database on the FDA website (www.fda.gov/foi/warning.htm). In addition, the sponsor should insert appropriate warranties in the clinical trial agreement to help it avoid engaging investigators, institutions, IRBs or ECs that have been disqualified or are under investigation by the FDA or its EU counterparts. GCPj

Katherine R Leibowitz,
Wim Nauwelaerts,
Hogan & Hartson,
Philadelphia, PA, US
Brussels, Belgium
Tel: +1 267 675 4612
E-mail: krleibowitz@hhlaw.com
E-mail: wnauwelaerts@hhlaw.com