Navigating the sea of data protection law in European clinical research

Clinical research is frequently carried out on a global scale. This globalisation presents a number of legal challenges, particularly where projects involve European partners since European data privacy laws place strict limitations on how individuals' personal data may be collected, used, and disclosed.

In Europe, there is a common set of rules that regulate the collection, use, and sharing of personal data. These include strict protection of sensitive data such as health data. However, individual European countries have interpreted and implemented the rules on the use of health data in clinical research, and possible exemptions from the rules, in very different ways. As a result, there is no uniform approach to managing clinical research data in Europe.

Any clinical research that involves the use of personal data must comply with the data protection rules. Although data protection laws try to strike a balance between an individual's right to privacy and the conduct of scientific research (from which society reaps important benefits), technological developments have led regulators to take a more expansive view of what constitutes personal data.

Under European data protection laws, personal data is any information that relates directly or indirectly to an identified or identifiable individual. When identification is impossible, i.e. where the data can be anonymised by permanently disassociating the information from the individual, such data is not considered to be personal data and therefore not subject to data protection rules.

While the use of anonymised data in clinical trials might appear to be the simplest solution, the reality is that technological advances have made full and irreversible anonymisation difficult to achieve. The use of advanced analytics in particular makes identification of individuals easier. A study published by the Carnegie Mellon University in 2000 (L. Sweeney, Uniqueness of Simple Demographics in the U.S. Population, LIDAPWP4. Carnegie Mellon University) showed that researchers were able to ascertain the identity of 87% of the US population using only their gender, ZIP code, and date of birth. Such combination of information is often used in clinical records to keep track of patients whose other details, such as name and address, are not recorded in an effort to anonymise data. Moreover, the lack of standard criteria for anonymising data makes the use of anonymous data less feasible.

Pseudonymisation, the disassociation of personal data from a data record and replacing it with a pseudonym or code, is another possible, albeit imperfect, solution. It entails fewer risks to an individual's privacy; however, because a pseudonym can be later tracked back to the source data record, the pseudonymised record may still be considered personal data because the individual can be indirectly identified. While some European countries provide for less onerous restrictions on the use of pseudonymised data, other countries apply the full range of data protection requirements even to data that has been pseudonymised.

Muddying the waters

Where health data cannot be anonymised or pseudonymised, for example when the research concerns a group of individuals with a very specific or rare medical condition, or when patient's identification does not cause disproportionate effort, data protection laws impose strict limitations on the use of such data. Most importantly, patients must be aware that their data will be used in the research and be informed about why their data are being collected. But when the research involves older medical records, finding the patients may not always be possible. Also, unless limited exemptions apply, individuals must explicitly consent to the use of their data. A general consent for an unspecified purpose is not sufficient. These restrictions can be onerous and do not always directly enhance

the protection of patient's privacy. Another complicating factor is that individuals have the right to withdraw their consent at any time. If consent is withdrawn, use of the data must cease immediately, adversely affecting the research project.

Another option is to rely on the exemptions for scientific research. When data are used for scientific purposes, most European countries exempt those activities from some or all of the data protection obligations. In such cases, consent is not required to use personal data for unrelated purposes if data are used for scientific purposes, but a number of countries impose varying additional obligations on the use of health data. For example, Austria and Italy impose security measures specific to the health sector, Italy requires that researchers follow the data protection authority's guidelines and Austria requires that health data be encoded. Belgium requires data anonymisation and approval from the data protection authority. Ireland, Slovakia, Poland and the UK require that the use of data not adversely affect individuals. In Germany, secondary use of data for research purposes is permitted if the scientific interest significantly outweighs the individual's interests. In contrast, Finland and the Netherlands do not impose additional safeguards for such secondary use.

Navigating the plethora of standards in search of a coherent approach may not always be easy or even possible. The problem is compounded when multiple parties such as clinical investigators, clinical research organisations, sponsors and monitors from different countries are involved because there is uncertainty about which laws apply.

The impact on research projects

Given these varied legal requirements, it can take several months to identify the data protection obligations and implement compliance measures. The more parties and different countries involved the more complex and lengthy the process will be. The costs of data protection compliance (providing notices, obtaining and recording any required consents, implementing security measures, and setting up a system for providing access) must be factored in to any clinical research study.

Failing to comply with European data protection laws can jeopardise a clinical research project. While not all laws are actively enforced, violations can lead to administrative and criminal penalties, including imprisonment. Over the last 18 months, the UK Information Commissioner has imposed several significant fines for data breaches including sensitive data; the Commissioner can issue maximum fines of £500,000. The Spanish government, able to levy some of the highest fines in the EU, issued more than 25 sanctions concerning the sharing of health data through peer-to-peer file sharing programs. Following its investigations, the Spanish data protection authorities imposed reporting requirements on public and private hospitals. The Italian data protection authority has recently announced a more stringent approach to enforcement concerning violations involving health data following several cases of misuse of data related to the sales of healthcare products.

Lawsuits for damages may follow, and many data protection authorities actively publicise non-compliance which can cause reputational damage. Most importantly, data protection authorities may halt the data processing, effectively putting a stop to an entire project. There is a growing tendency for data protection authorities to pursue active investigations and enforcement rather than merely ensuring oversight privacy compliance. Therefore, addressing these requirements before undertaking a research project is a crucial element in the success of a project.

Solutions to address compliance

The benefits of research must be weighed against the risks associated with use of health data. A multilayered approach should be considered. If anonymised data cannot be used, the project managers should consider whether the use of pseudonymised data with appropriate safeguards is possible. Otherwise, consent from affected individuals may be necessary. Any consent must be specific to the research project in question unless the consent obtained at the time of initial collection expressly covered use for research purposes at a later date.

There is a growing need for more clear-cut data protection rules that will facilitate rather than impede this research.

Compliance may be less onerous if key steps are built into the research project in phases:

- Initial phase: Identify what personal data will be used in the project, and assess whether it is possible to anonymise or pseudonymise the data. Identify the data protection responsibilities of the partners involved in the project. In countries where sectoral codes (Spain) or data protection guidelines (Italy) exist, implement this guidance to obtain a consistent approach and reduce the level of uncertainty with respect to interpretation of the law.
- Implementation phase: Obtain individuals' explicit and specific consent to use data where they cannot be anonymised. Before obtaining consent, individuals must receive information about the type of data to be collected and the purposes of use. Technical and organisational security measures will be required to protect against accidental loss of or unauthorised access to the data.
- Data disclosure: If data will be shared with other research partners, put written contracts into place that require third parties to adhere to high security standards and limit data use to prescribed purposes. These contracts will vary depending on the destination country and the role of the data recipient.
- Registrations: Register or obtain data protection authority approvals before data are collected and transferred.

The need for change

Globalisation has brought new opportunities and challenges to organisations engaged in clinical research. There is a growing need for more clear-cut data protection rules that will facilitate rather than impede this research. Overly burdensome regulation will simply discourage these organisations from conducting such projects in Europe.

Clearer rules on applicable law, unified exemptions for the use of data for scientific purposes, and standard information notice and consent forms would encourage and facilitate the conduct of clinical research. Mutual recognition of approved privacy standards for research projects or at least standard approval procedures would also greatly contribute to reducing this regulatory burden.

Karin Retzer is Of Counsel at Morrison & Foerster, Brussels; Joanna Łopatowska is an associate in the Privacy and Data Security Group in Morrison & Foerster, Brussels; and Cynthia Rich is a senior international policy analyst at Morrison & Foerster LLP, Washington DC, USA.