Bloomberg BNA

Medical Research Law & Policy Report®

European Union's Proposed General Data Protection Regulation Promises Big Changes for Secondary Uses of Data from Clinical Trials




By David Peloquin, Sarah Ferranti, Sabrina Ross and Mark Barnes

On Oct. 21, 2013, in the latest stage of reform of data privacy laws in the European Union ("EU"), the European Parliamentary Committee on Civil Liberties, Justice, and Home Affairs ("LIBE") voted to approve amendments to the General Data Protection Regulation (as approved by LIBE, the "2013 GDPR"), which initially had been proposed by the European Commission in January 2012. The GDPR is intended to supersede in full the current Directive 95/46/EC of the European Parliament ("1995 Directive"), which was adopted in 1995 and then transposed into a broad array of national laws by EU Member States.[1] Unlike the 1995 Directive, the 2013 GDPR, which has the higher status of an EU-wide "Regulation," will require each member state to implement its exact language into national law, promising greater consistency and predictability for regulated entities.

Now that it has been approved by the LIBE, the 2013 GDPR will be subject to review by the European Council. Unless substantial changes are adopted by the Council, the final version of the Regulation may have the effect of significantly complicating and hindering research involving health data, including secondary research uses of data.

David Peloquin, Sarah Ferranti, Sabrina Ross and Mark Barnes are attorneys at Ropes & Gray LLP. Mark Barnes teaches at Harvard Law School and serves as the faculty co-director of the Multi-Regional Clinical Trials (MRCT) Center at Harvard.

[1] *See* Council Directive No. 95/46/EC 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, O.J. L. 281/31 (1995) [hereinafter "1995 Directive"].

 ISSN 1539-1035

Status of Pseudonymised and Encrypted Data

Research generally necessitates one of three categories of subject data: identifiable data, pseudonymised or encrypted data, or fully anonymised data. Pseudonymised and encrypted data are particularly beneficial for secondary analyses, as they allow researchers to evaluate subject-level data while protecting individual privacy.

The 1995 Directive and the 2013 GDPR both regulate ''personal data''—information relating to an identified or identifiable natural person, meaning a person who can be identified directly or indirectly, in particular by reference to one or more identifiers of that person.[2] The 1995 Directive does not, however, address whether ''personal data'' include pseudonymised or encrypted data; consequently, individual EU Member States have imposed inconsistent rules about the treatment of such data. The 2013 GDPR clarifies for the first time that pseudonymised or encrypted (*e.g.*, key-coded or hashed data) *are* considered to be ''personal data,'' in contrast to fully anonymised data.[3] Data will be considered anonymised (and not subject to the GDPR's restrictions) only if they consist of ''information that does not relate to an identified or identifiable natural person.''[4] If the final adopted version of the 2013 GDPR retains these LIBE-adopted definitions of pseudonymous and anonymised data, the use of key-coded or encrypted clinical trial numbers or any other identification numbers that link back to the identity of the subject, regardless of whether they are derived from other personal information about the subject, will be subject to the same requirements as other types of personal data.

Consent Requirements

Also of significance to those conducting research on data gathered in clinical trials are the ways in which the 2013 GDPR would strengthen consent requirements. Like the 1995 Directive, the 2013 GDPR would impose a general prohibition on the processing of certain varieties of sensitive personal data, including data concerning health.[5] The 2013 GDPR provides for a number of exceptions to the general prohibition, including exceptions for processing sensitive data (a) with consent of the data subjects; (b) when necessary for health purposes subject to the conditions and safeguards referred to in Article 81 (Processing of Personal Data Concerning Health); or (c) when necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83 (Processing for Historical, Statistical and Scientific Research Purposes).

Article 81 would permit the ''processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes . . . only with the consent of the data subject, and . . . subject to the conditions and safeguards referred to in Article 83.''[6] Article 83, in turn, would permit the processing of personal data for historical, statistical or scientific research purposes only if:

(a) the purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject; *and*

(b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information under the highest technical standards, and all necessary measures are taken to prevent unwarranted re-identification of the data subjects.

Taken together, the above provisions suggest that processing of data concerning health for scientific research could be performed only when (1) the data subject has provided his or her consent; *and* (2) the data are anonymised or pseudonymised as soon as possible, consistent with the research purposes. This second conclusion comes from the requirement in Article 83 that data permitting re-identification of the subject must be kept separately from the other information under the ''highest technical standards,'' thereby suggesting that when anonymisation of data is not possible, the data should at least be encrypted or pseudonymised.

The LIBE-adopted Article 81 introduces the possibility that individual Member States will be able to create *additional* exceptions to the requirement of consent for research that involves the processing of personal data concerning health. Specifically, Article 81 provides that Member States may create an exception to the consent requirement for research that: (1) serves a ''high public interest''; (2) cannot be carried out otherwise; and (3) involves data that have been anonymised, or if not possible, pseudonymised under the ''highest technical standards.''[7]

While the 2013 GDPR does not elaborate on what constitutes a ''high public interest,'' there is some evidence to suggest that research concerning health may fall into this category. The 1995 Directive employed the

[2] 2013 GDPR, Article 4, paragraph 2.

[3] ''Pseudonymous data'' are defined as ''personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution.'' Article 4, paragraph 2a. ''Encrypted data'' on the other hand are defined as ''personal data, which through technological protection measures is rendered unintelligible to any person who is not authorized to access [them].'' 2013 GDPR, Article 4, paragraph 2b.

[4] 2013 GDPR, Recital 23.

[5] Under the 2013 GDPR, ''data concerning health'' means any personal data information which relates to the physical or mental health of an individual, or to the provision of health services to the individual. 2013 GDPR, Article 4.

[6] The 2013 GDPR does not itself define what constitutes historical, statistical or scientific research purposes. Additional gloss on these terms has been provided in guidance issued by the EU's Article 29 Data Protection Working Party. This guidance suggest that *historical research* covers processing of data for national archives or court files; *statistical research* covers processing for commercial purposes, market research, use of analytical tools of websites and public interest research; and *scientific research* covers fundamental research, applied research and privately funded research. Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 00569/13/EN WP 203, at 29 (2 April 2013), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[7] 2013 GDPR, Article 81, paragraph 2a. The 2013 GDPR also suggests that in the future such an exception may be created on an EU-wide basis, noting that ''the processing of personal data concerning health, as a special category of data, may be necessary for reasons of historical, statistical or scientific research. Therefore, this Regulation foresees an exemption from the requirement of consent in cases of research that serves a high public interest.'' *See id*. Recital 123a.

  MRLR ISSN 1539-1035

term ''substantial public interest'' and included within the definition of that term ''promotion of public health.''[8] The 2013 GDPR indicates that ''public health'' should be defined according to Regulation 1338/2008,[9] which in turn defines public health as ''all elements related to health.'' Accordingly, if one assumes that the terms *substantial* and *high* are synonymous in this context, research activity that qualifies as a substantial public interest also may qualify as ''high public interest'' under the 2013 GDPR.

While the ''high public interest'' exception therefore does provide some hope for flexibility on the consent requirement (particularly when consent is impossible or infeasible), its application is uncertain at best, and undertaking medical records or similar data research would still require complying with numerous inconsistent Member State laws, contrary to the GDPR's ''one continent, one law'' aim.

Conditions of Consent for Research Uses of Personal Data

The conditions of consent proposed by the 2013 GDPR further complicate the use of clinical trial data for secondary research analyses. The 2013 GDPR defines the ''data subject's consent'' as ''any freely given specific, informed, and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.''[10] For sensitive data, including data concerning health, genetic data or biometric data, the 2013 GDPR further provides that consent for processing must be for one or more specified purposes, subject to the conditions in Article 7 (Conditions for Consent) and Article 8 (Processing of Personal Data of a Child), except as otherwise prohibited by EU law or Member State law.[11] Likewise, 2013 GDPR Article 81, paragraph 1b, provides that consent may be given for ''one or more specific and similar researches.''

While the 2013 GDPR does not define the term ''specific,'' guidance from the Article 29 Data Protection Working Party, an organization established by the 1995 Directive to act in an advisory capacity regarding data protection issues, indicates that to be ''specific,'' the consent must be ''intelligible,'' *i.e.*, ''it should refer clearly and precisely to the scope and the consequence of the data processing. It cannot apply to an open-ended set of processing activities.''[12] In another context, the Article 29 Working Party has provided the following as examples of data collection that are too vague to be considered ''specific'': ''improving users 'experience,' 'marketing,' 'IT-security' or 'future research.' ''[13]

The requirement that consent be ''specific'' therefore is potentially highly problematic for those researchers and commercial or not-for-profit entities conducting secondary research using clinical trials data. Researchers often try to obtain ''broad consent'' in the informed consent used for a given clinical trial or other research study, in order to permit a wide variety of future uses to be made of data and specimens collected during the trial or study. However, through its use of the word ''specific'' and the previous EU interpretations of that term to preclude consent for ''future research,'' the text of the 2013 GDPR is inconsistent with the common practice of obtaining broad consent for future research uses. Significantly, prior to the LIBE's consideration of the GDPR in October 2013, the scientific research and pharmaceutical community had lobbied the LIBE for several proposed amendments that explicitly would have permitted data subjects to give ''broad consent'' or a ''one-time consent'' to facilitate future research on data collected in clinical trials.[14] These amendments were uniformly rejected by the LIBE.[15] Given the requirement of ''specific'' consent, it is unclear whether consent language related to future research, such as language through which the data subject allows for future research related to the study disease or related to any disease, would be permissible, if the 2013 GDPR is adopted in its current form.

Right to Erasure

Through its establishment of a ''right to erasure,''[16] the 2013 GDPR also may pose challenges for future research on personal data. Under U.S. law, if a research subject exercises the right to withdraw permission for his or her health information to continue to be used for research purposes, researchers may continue to use and disclose such information obtained prior to the revocation of the permission, insofar as necessary to ''maintain the integrity of the research study.''[17] The 2013 GDPR's ''right to erasure'' requires that if the data subject withdraws the consent on which the processing

[8] *See* 1995 Directive, Recital 34.

[9] *See* Regulation (EC) No 1338/2008 of the European Parliament and of the Council, of 16 December 2008, on Community statistics on public health and health and safety at work.

[10] 2013 GDPR, Article 2, paragraph 8.

[11] 2013 GDPR, Article 9(2)(a).

[12] Article 29 Working Party Opinion 15/2011, at 17.

[13] Article 29 Working Party Opinion 3/2013, at 52.

[14] *See* Roundtable Event Hosted by Nessa Childers MEP, *Data Protection Regulation: Keeping Health Research Alive in the EU*, Sept. 17, 2013, page 5, http://www.feam-site.eu/cms/docs/activities/DPR/JointWorkshopDPR_17September2013_Report.pdf.

[15] Two examples of proposed amendments to Article 83 that were rejected include the following:

''The data subject has given his or her consent for the processing of data for historical, statistical and scientific research. For the purposes of historical, statistical and scientific research, a one-time consent is enough and there is no need for explicit consent to be given each time by the data subject, or a need to notify the data subject, separately before the processing of data related to research purposes.'' *See* Amendment 3067, *in* Jan Phillip Albrecht, Amendments (10) 2951-3133, on the proposal for a regulation (COM(2012)0011-C7-0025/2012-2012/0011(COD)), March 8, 2013, *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/am/929/929832/929832en.pdf.

''A data subject should always have the option to give broad consent for his or her data to be used for historical, statistical or scientific research purposes, and to withdraw consent at any time.'' *See* Amendment 498, *in* Jan Phillip Albrecht, Amendments (1) 351-601, on the proposal for a regulation (COM(2012)0011-C7-0025/2012-2012/0011(COD)), March 4, 2013, *available at* http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/am/926/926396/926396en.pdf.

[16] *See* 2013 GDPR, Article 17.

[17] *See* National Institutes of Health, *HIPAA Privacy Rule for Researchers: Frequently Asked Questions* (FAQ# 20), http://privacyruleandresearch.nih.gov/faq.asp; 45 C.F.R. § 164.508(b)(5)(i).

of personal data is based, the data controller must erase personal data concerning the subject, abstain from further dissemination of such data, and obtain from third parties the erasure of any links to, or copy or replication of, the data.[18]

Under the 2013 GDPR, subjects may not be able to exercise their ''right to erasure,'' if retention of the personal data is necessary for ''historical, statistical and scientific research purposes in accordance with Article 83'' or ''for reasons of public interest in the area of public health in accordance with Article 81.''[19] At present, it is unclear how broadly these restrictions on the ''right to erasure'' will be construed. As discussed above, the LIBE has tried to protect subject rights by regarding as ineffective any broad consent to future research uses of personal data. Accordingly, to the extent there are restrictions on the ''right to erasure'' for personal data used in research, it seems unlikely that the LIBE would favor any barrier to subjects being able to exercise that right and thus prevent future research uses of their personal data. Researchers therefore would need to comply with any request for erasure from a data subject, thus preventing any use of those data for later secondary research.

Enhanced Penalties

The 2013 GDPR would increase penalties for failing to comply with data protection requirements to include: (1) regular data protection audits by a governmental agency; and/or (2) fines that can be as high as the greater of 5 percent of an enterprise's annual worldwide revenue or 100 million Euros.[20] In determining the penalty to be imposed in a particular case, the enforcing agency shall take into account: (a) the nature, gravity and duration of the non-compliance; (b) the intentional or negligent character of the infringement; and (c) the specific categories of personal data affected by the infringement.[21] The 2013 GDPR additionally creates a private right of action for individuals who have suffered damage, including non-pecuniary damage, resulting from violations of the 2013 GDPR.[22]

Conclusion

While the 2013 GDPR likely will undergo additional changes prior to becoming EU law, the draft approved by the LIBE in October 2013 would place severe restrictions on the use of clinical trials and other primary research data for future secondary research. Researchers and entities conducting or sponsoring studies in the EU Member States should closely monitor the progress of the GDPR as it is finalized, paying particular attention to further clarifications regarding the treatment of pseudonymised and encrypted data, specificity of consent required for processing of data related to health, and the scope of the ''right to erasure.'' If passed in its present form, attention may next turn to the EU Member States, as they begin to define what types of research on personal data will qualify as a ''high public interest,'' thus enjoying a potential exemption from the new, more rigorous consent requirement.

---

[18] *See* 2013 GDPR, Article 17, paragraph 1.
[19] *See id*. paragraph 3(b), (c).
[20] *See* 2013 GDPR, Article 79.
[21] *See id*. paragraph 2c.
[22] *See* 2013 GDPR, Article 77.

   ISSN 1539-1035