Bloomberg Law

Medical Research Law & Policy Report®

Extraterritorial Effect of the GDPR and Implications for U.S. Academic Medical Centers Treating EU Patients

By Tim McCrystal, Rohan Massey, David Peloquin, Nicholas Wallace, and Mark Barnes

When it takes effect on May 25, 2018, the European Union (''EU'') General Data Protection Regulation will impose stringent data protection requirements on entities that process ''personal data.'' (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter the ''GDPR'')). Many U.S.-based health care entities that treat patients who are resident in the EU, that have other business or professional relationships with EU entities and residents, and/or that interact with and gather personal data from research subjects, are understandably eager to avoid becoming subject to the GDPR's requirements. U.S. entities should therefore be aware that the GDPR applies extraterritorially in a greater number of situations than the currently effective EU Data Protection Directive. (EU Data Privacy Directive (Directive 95/46/EC) (hereinafter the ''Directive'')).

In particular, this article considers the possible extraterritorial application of the GDPR to data held by U.S. health care providers in their medical records relating to the care of individuals residing in the 28 member states of the EU and the three additional countries (Iceland, Liechtenstein, and Norway) that together with the EU make up the European Economic Area (''EEA'') to which the Directive and GDPR apply. We focus in particular on U.S. academic medical centers (''AMCs''), which treat a significant number of international patients as a result of such AMCs' preeminence in certain medical fields and which may, in certain cases, maintain formal consultative, referral, or other professional and business relationships with EEA health care providers.

Tim McCrystal, Rohan Massey, David Peloquin, Nicholas Wallace, and Mark Barnes are attorneys with Ropes & Gray LLP.

Jurisdictional Scope of the GDPR Compared with the Directive

The GDPR will supersede the presently effective Directive, which was adopted in 1995. (*See* Directive). In contrast to the GDPR, which will be directly effective in all of the EEA's member states, the Directive did not directly regulate privacy practices but instead required that the member states of the EEA transpose its principles into their national bodies of law, creating legal divergences across the EEA. (*See* Directive).

With respect to its jurisdictional reach, the Directive applies only to organizations that (i) collect and/or use personal data if such organizations are established within the EEA and process personal data in the context of such establishments; (ii) are established outside the EEA, but use equipment within the EEA to process personal data (unless such equipment is used only for transit purposes); or (iii) process data in a place where an EEA member state's law applies ''by virtue of public international law.'' (Directive Art. 4). The Directive, therefore, has applied to U.S.-based AMCs only in those scenarios in which an AMC is ''established in'' the EEA by, for example, operating a subsidiary or campus in the EEA or using equipment in the EEA to process personal data. The third jurisdictional category under the Directive is intended for instances in which international law determines the application of data protection law, such as in the case of data processing by a foreign embassy or consulate, or data processing that occurs on

a ship or airplane, circumstances which would be unlikely to apply to an AMC.

The GDPR, however, significantly expands the territorial scope and ''long arm'' reach of EU data protection law. Under the GDPR, ''personal data'' are defined broadly as:

''[A]ny information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.'' (GDPR Art. 4(1)).

By its terms, the GDPR may apply to certain non-EU organizations that process personal data of EEA data subjects outside of the EEA. Specifically, the GDPR's text states that it applies when:

1) Personal data are processed in the context of activities of an establishment of a controller or a processor in the EEA, regardless of whether or not the processing takes place in the EEA;

2) An organization that is not established in the EEA processes data (i) in the context of offering goods or services to data subjects located in the EEA or (ii) the monitoring of the behavior of data subjects as far as the behavior takes place within the EEA; or

3) Personal data are processed by a controller not established in the EEA, but in a place where the national law of an EEA member state applies by virtue of public international law. (*See* GDPR Art. 3).

While the first and third categories of data processing to which EU data protection law applies remain similar to those that exist under the present Directive, the second category of processing could result in additional circumstances in which EU data protection law would apply to U.S.-based AMCs treating patients from the EEA.

Potential Extraterritorial Application to U.S. AMCs

In order to further the reach of their specialty physicians and services, AMCs increasingly treat patients from beyond the borders of the U.S., including through referral or consultative relationships with EEA health care providers. Some such arrangements may provide opportunities for foreign hospitals and physicians to consult remotely with the AMC specialists regarding diagnosis and treatment issues and, in certain cases, to refer patients to the AMC for specialized diagnostic review or treatment. As analyzed in this section, the GDPR's second category of covered data processing could be read to include extraterritorial data processing in connection with such referrals or consultations.

To date, there has been a lack of guidance clarifying when organizations not established in the EEA will be considered to be ''offering goods and services to data subjects'' located in the EEA or ''monitoring the behavior of data subjects'' within the EEA. The concern for AMCs with consultative and referral relationships with EEA hospitals is that establishing a formal referral relationship with an EEA hospital or an ongoing consultative relationship with EEA hospitals or physicians regarding patient care could be construed as ''offering goods or services to data subjects'' within the EEA or ''monitoring the behavior of data subjects.'' If the actions were deemed to meet the definition, the GDPR would apply to the AMC's processing of the EEA patients' personal data in the U.S. Such personal data could include detailed notes taken by AMC physicians in the course of consultative discussions with European colleagues or the medical records of EEA persons who are referred to the AMC for care. The U.S. AMC would bear the burden of identifying the personal data to which the GDPR applies and ensuring compliance with the GDPR's requirements.

'Offering Goods or Services' to Data Subjects in the EU

The GDPR itself provides limited clarity regarding the interpretation of ''offering goods or services'' to data subjects within the EEA, especially with respect to the types of personal data likely to be processed by AMCs. To the extent that the GDPR provides clarity, it is with regard to factors that could be construed toward considering an AMC's consultative or referral relationships to be ''offering goods or services'' to EEA data subjects. First, the GDPR notes that the goods or services offered should be considered ''irrespective of whether connected to payment.'' (GDPR, Recital 23). Thus, an AMC's consultative and referral relationships could be swept into the ambit of the GDPR even if the AMC does not charge the EEA patients for the consultative services and does not charge EEA patients for services provided at the AMC itself. Second, the GDPR provides that, ''[i]n order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union.'' (*Id.*). Because AMCs' relationships with European health care providers are likely to be governed by a written agreement or to be established through routine practice, it could be possible to view such relationships as the AMC's ''envisioning'' that it is offering or will offer services to EEA data subjects, and this factor similarly could be interpreted to subject the AMC to the GDPR with respect to the personal data it holds of such individuals. Moreover, it should be remembered that under the GDPR, it is not solely the personal data of EEA patients that are protected, but also the data of the *EEA health care providers themselves*, because even the names and other identifying information of health care providers, not just patients, are protected under the GDPR. Therefore, even if an AMC could argue that through offering a consultation service to an EEA health care provider it does not offer a good or service directly to an EEA *patient*, the AMC could be seen as providing a good or service to an EEA *health care provider,* who is also by definition an EEA *data subject*, thereby triggering obligations under the GDPR toward these individual providers.

While the above suggests that a formal or repetitive consultation relationship between an AMC and EEA health care providers could be seen as ''offering goods or services to data subjects in the [EEA],'' it should be noted that the GDPR also suggests that occasional treatment of subjects from the EEA who travel to the U.S. to seek services at the AMC or occasional informal consultation between the AMC and EEA health care providers may not give rise to application of the GDPR. Specifically, in discussing when an ex-EU data control-

   ISSN 1539-1035

ler ''envisages offering services to data subjects in one or more [EEA Member States],'' the GDPR's recitals clarify that ''mere accessibility of the controller's, processor's or an intermediary's website'' in the EEA is insufficient in and of itself to ascertain such intention. (***Id.***). Rather, the GDPR suggests that in order to subject themselves to GDPR jurisdiction through their website activity, data controllers not established in the EEA would need to take an additional step to direct their website to EEA data subjects, such as translating their website into a foreign language or mentioning customers or users in the EEA. Thus, by analogy, if an AMC does not establish a formal or repetitive arrangement with an EEA health care provider or target its advertisements directly to EEA patients or health care providers, an AMC may not be seen as offering goods or services to EEA data subjects, even if the AMC on occasion treats EEA patients or offers consultation services to EEA health care providers.

Telemedicine and 'Monitoring Behaviour' of EEA Residents

The GDPR's text is similarly unclear as to whether ''monitoring behaviour'' of data subjects could encompass an AMC's consultative or referral relationships with EEA hospitals and patients or an AMC's sponsoring or coordination of a clinical trial at EU sites. The GDPR's recitals provide that ''[i]n order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.'' (GDPR, Recital 24).

An AMC's consultative relationship with an EEA health care provider would appear generally not to include the type of activity contemplated by the recital, given its emphasis on the tracking of behavior on the internet to predict preference or behaviors. However, if the consultative relationship involves the interaction of a U.S.-based physician through telemedicine with a patient located in the EEA, the consultation may be more likely to be subject to scrutiny as potential ''monitoring'' of the behavior of EEA data subjects.

Similarly, if an AMC sponsors a clinical trial with sites located in the EU, certain activities could arguably constitute ''monitoring of the behaviour of data subjects.'' For example, in certain research studies a sponsor or coordinator might have direct contact with research subjects, for example, by providing consultation with the subjects directly via telephone or videoconferencing technology. Such direct interaction with data subjects could arguably be considered ''monitoring behaviour'' such that the AMC's processing of personal data from the trial would be subject to the GDPR. Where a U.S. AMC serves only as a coordinating center that merely processes coded data (referred to as ''pseudonymised'' data under the GDPR) that have been collected by EU study sites and then transferred to the AMC, it seems less likely that the AMC would be seen as ''monitoring'' the behavior of the EU study subjects directly thereby triggering direct application of the GDPR. However, even if the AMC is not seen to be ''monitoring'' the behavior of the EU study subjects, a legal basis to legitimize the transfer of the personal data from the EU to the U.S. would be required, as discussed below under ''Additional Considerations.''

Recent EU Commentary on Extraterritorial Reach of GDPR

EU officials have noted the lack of clarity surrounding the GDPR's extraterritorial application, and particularly the application of the GDPR on the basis of ''offering goods or services'' to persons located in the EEA. However, to the extent that EU officials have weighed in on the vagueness, they have often encouraged broad construction of such phrases.

The Article 29 Data Protection Working Party, the EU body that provides non-binding guidance on EU data protection law, issued an opinion on the data protection reform proposals prior to the finalization of the GDPR in which it called for greater clarity regarding the key terms by which extraterritorial jurisdiction could arise:

''Notwithstanding attempts to define what is meant by both 'offering of goods and services' and 'monitoring of their behaviour' in the recitals, the Working Party feels further clarification of these notions would be helpful.'' (Article 29 Data Protection Working Party, Opinion 01/2012 on the Data Protection Reform Proposals 9 (Mar. 23, 2012)).

Notably, however, the Working Party's proposals on the draft regulatory changes were to broaden, rather than narrow, the potential scope of the vague phrases:

''It should be made clear that the 'offering of goods and services' also includes free services (where individuals in fact pay for the service by providing their personal data). The Working Party therefore suggests adding wording along the lines '*including services provided without financial costs to the individual.*' Furthermore recital 21 implies that 'monitoring of behaviour' is linked to tracking on the internet and creating profiles. The Working Party advises to change the wording in order to ensure that even if the controller does not create profiles as such, processing activities can sometimes be considered 'monitoring of behaviour' if they lead to decisions concerning a data subject or involve analysing or predicting his or her personal preferences, behaviours and attitudes.'' (*Id.*).

The European Data Protection Supervisor also has issued formal recommendations on the EU data protection reform proposals, which included an acknowledgment that ''[t]he material and territorial scope of the GDPR is difficult to summarise succinctly.'' (Recommendations of the European Data Protection Supervisor: EDPS Recommendations on the EU's Options for Data Protection Reform (2015/C 301/01, 06, note 7)). However, the Supervisor noted, without further elaboration, that the EU governing institutions ''seem to agree, at least, that the scope covers organisations established in the EU . . . [and] organisations established outside the EU who process personal data of individuals in the EU in the course of offering goods or services to or monitoring individuals in the EU.'' (*Id.*). Thus, while acknowledging the complexity of the matter, the Supervisor did not provide greater clarity as to the interpretation of the standards causing, at least in meaningful part, that complexity.

As the GDPR enforcement date moves closer, additional guidance clarifying the scope of the regulation's jurisdictional hooks may be issued. Such guidance could provide welcome clarity. In crafting guidance, it

would be helpful for EU regulators to take into account the particular nature of professional consultative and referral relationships and the risk to EEA persons of a chilling of such relationships by an interpretation of the GDPR that would apply GDPR protections to personal data created in the course of such relationships. In the meantime, AMCs should take a close look at their relationships with European organizations to evaluate the likelihood that they could be subject to the GDPR's data protection regime.

Additional Considerations

AMCs should be aware that, while the above analysis examines the impact of the GDPR on AMCs' U.S. operations, both the Directive currently in effect and the GDPR, upon its implementation, require that a legal basis be in place to permit the transfer of personal data concerning a data subject from the EEA to the U.S. This is because both the Directive and the GDPR require that personal data not be transferred from the EEA to countries that have been determined by the European Commission to lack adequate data protection regimes, such as the U.S., absent the presence of a legal basis to legitimize the transfer. Accordingly, when personal data are transferred from the EEA to the U.S. for processing, a legal basis for such transfer is needed under both the Directive and the GDPR. (*See* Directive Ch. IV; GDPR Ch. V). In the context of an AMC's activities, this legal basis may occur through (i) obtaining the unambiguous consent of the data subject to the transfer of personal data to the AMC for processing, or (ii) through the AMC entering into one of the model contractual clauses approved by the European Commission with the entity transferring the data to the AMC. These contractual clauses impose on the contracting AMC certain of the requirements of EU data privacy law with respect to the data transferred pursuant to the contract. AMCs that are for-profit entities may have an additional option available to them, in that they may be able to apply for certification under the Privacy Shield, a program administered by the U.S. Department of Commerce that permits personal data to be transferred from the EEA to U.S. entities that self-certify for the program after implementing various data protection measures. Therefore, even if an AMC's activities do not subject it directly to regulation under the GDPR, the AMC may be required to take measures to ensure that an adequate legal basis exists to permit the transfer of data from the EEA to the U.S. for the AMC's treatment activities.

Implications of GDPR's Application to U.S. AMCs

If an AMC's activities become subject to the GDPR, there are a number of domains in which the GDPR imposes heightened requirements beyond those with which most U.S. AMCs are required to comply under the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (''HIPAA''). First, the GDPR contains no safe harbor for anonymization akin to the HIPAA Privacy Rule's de-identification safe harbor, rendering anonymization a facts and circumstances test that is generally more difficult to achieve than de-identification under the HIPAA safe harbor. (*See* GDPR Art. 4(1); 45 C.F.R. § 164.514(b)). Second, the GDPR provides for a broader data subject access right than does HIPAA. The GDPR will allow data subjects to obtain copies of all of their personal data undergoing processing, whereas HIPAA provides a right of access only to protected health information stored within a covered entity's ''designated record set'' and contains exceptions for certain categories of PHI including psychotherapy notes or PHI collected during a research study provided that the subject agreed to the suspension of the right of access for the pendency of the research. (*See* GDPR Art. 15; 45 C.F.R. § 164.524). Similarly, the GDPR provides the data subject the right to obtain additional information in an accounting of disclosures, including the source of the personal data where the source is not the data subject. (*See* GDPR Art. 15; 45 C.F.R. § 164.528). In addition, the GDPR contains a ''right to erasure,'' also known as a ''right to be forgotten,'' that permits the data subject to request that data be erased under any one of six circumstances, including when the subject withdraws consent on which the processing is based. (*See* GDPR Art. 17).

Third, the GDPR also imposes a number of procedural requirements not present under HIPAA, including a requirement that data controllers consult with EU supervisory authorities prior to processing when the processing would result in a high risk and the controller has not implemented measures to mitigate the risk. (*See* GDPR Art. 36). Likewise, the GDPR requires non-EU data controllers and processors subject to the GDPR to appoint an EU representative unless their processing is occasional and certain other requirements are met. (*See* GDPR Art. 27). Fourth, with respect to enforcement penalties, fines from infringements under the GDPR can be extensive, with fines up to the higher of €10,000,000 or 2 percent of worldwide annual turnover for the violation of some provisions and the higher of €20,000,000 or 4 percent of worldwide annual turnover for violation of other provisions, including the provisions on subject access and right to erasure. (*See* GDPR Art. 83). Fifth, unlike HIPAA, the GDPR confers a private right of action on data subjects, who may bring damages claims directly against data controllers and processors. (*See* GDPR Art. 82). In some jurisdictions, including the United Kingdom, individuals need only show distress in order to claim financial damages, so financial loss is not a determinative factor in the risk analysis.

Recommended Steps

Before the GDPR's effective date of May 25, 2018, it would be prudent for U.S. AMCs to take steps to identify their interactions with EEA health care providers and patients in the course of treatment activities. Such AMCs will want to consider whether such interactions are subject to a formal affiliation arrangement or result in repetitive interactions with EEA health care providers, or whether such arrangements occur on more of a sporadic basis as EEA health care providers consult with the AMC or EEA patients travel to the U.S. to seek treatment.

AMCs will also want to understand what mechanisms are currently in place to legitimize any transfer of patient data from the EEA to the U.S., and whether any updates to such mechanisms are needed as the GDPR compliance date moves closer and EEA entities increase their focus on instituting appropriate data protection measures. In addition, AMCs should monitor whether EU regulatory bodies issue further guidance clarifying the circumstances in which the GDPR applies to cross-border treatment activities.

   ISSN 1539-1035