Connecting Healthcare with Legal Excellence℠

Health Law Diagnosis

APPLICATION OF THE GENERAL DATA PROTECTION REGULATION (GDPR) TO THE TREATMENT OF EUROPEAN PATIENTS

This edition of Health Law Diagnosis (HLD) reviews and evaluates whether and under what circumstances Regulation 2016/679 of the European Parliament and of the Council 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 (the General Data Protection Regulation or "**GDPR**") applies to the delivery of health care and related services by United States' health care providers. Specifically, this edition of HLD evaluates whether the GDPR applies to health care services provided to a resident, national or other individual from the European Union ("EU") while such individual is located within the United States, as well as whether the GDPR applies to any other processing of data once the individual returns to the EU.

In short, the potential for GDPR applicability to a health care provider's operations appears to extend only to certain limited activities conducted in relation to individuals ***who are located within the EU at the time of the activity*****.** Where the risk is identified, although not high, if these activities can be reduced, a health care provider should attempt to do so where practicable. However, if it would not be possible to identify and/or reduce the occurrence of all such activities in relation to EU individuals, the likelihood of enforcement at this time with respect to a solely U.S. based health care provider such as a health care provider conducting these activities is very low. Furthermore, bringing a U.S. based health care organization into compliance with the GDPR could result in non-compliance with U.S. laws and regulations, such as state or federal laws which may mandate that a health care provider take certain action regarding data or disclose such data in a manner which would not be recognized by the GDPR structure. Therefore, it would not be advisable at this time for a health care provider to re-structure its operations for compliance with the GDPR unless or until such time as a health care provider conducts more specific and targeted activities in relation to the jurisdictional reach and scope of the GDPR.

GDPR Background

The GDPR harmonizes data protection laws across the EU and governs the processing of personal data. Compliance is imposed primarily upon "**data controllers**"; however, "**data processors**" are also independently subject to the GDPR. For purposes of the GDPR, the following key definitions apply:

- "**Personal data**" means any 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.[1]

- "**Processing**" means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation [sic], structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[2]

- "**Data controller**" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller (or the criteria for nominating the controller) may be designated by those laws.[3]

- "**Data processor**" means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.[4] A data processor provides functions similar to that of a "business associate" as described under the Health Insurance Portability and Accountability Act ("HIPAA").

Notably, the GDPR does not apply to all persons or organizations who or which process personal data, but to those that are "*established*" within the EU, and which process personal data of an *individual who is located within the EU* in the context of that establishment (*whether or not the actual processing occurs within the EU*). Where the data controller or processor is NOT established within the EU but is located outside of the EU (i.e., a United States health care provider), the GDPR would still apply, regardless of whether the processing occurred within the EU or without, if the controller or processor is:

- **offering goods and services to an individual located within the EU** (this includes offering services in the languages or currencies used in a Member State, mentioning customers/users in a Member State in advertisements, marketing activities., etc.). Passively accepting an EU resident as a customer or patient in the U.S. would not generally trigger the GDPR nor would the mere accessibility of the controller or processor's website, email and other contact detail, or use of a language generally in the country where the controller is established; or
- **monitoring the behavior of individuals located within the EU** (i.e., monitoring IP traffic, cookies, etc. through a website).

[1] Rec.26; Art.4(1). Personal data includes "special category data", which includes race, ethnic origin, politics, religion, trade union membership, genetics, biometric (if used for ID purposes), health, sex life, sexual orientation. Special categories of data require not only a lawful basis but also satisfaction of specific conditions prior to processing.
[2] Art.4(2)
[3] Art.4(7)
[4] Art.4(8)

Therefore, a health care provider providing care within the United States that ***does not actively seek or market health care services to patients from the EU*** (in contrast with a health care provider that may hold itself out to and actively seek to obtain patients from EU regions or a research institution which seeks international participants) and happens to provide treatment if the patient seeks care at the provider while visiting the U.S., would **not** generally be subject to the GDPR where the services are offered within the U.S. and the patient is **not within the EU** at the time the service is provided.

However, certain activities could still potentially trigger the GDPR, as discussed further hereing. These include the provision of ***post-discharge services*** and ***certain website functionality*** where the website monitors traffic and other visitor actions. Where the GDPR would apply, key principles of the GDPR would govern any offering of services or monitoring of behavior related to individuals within the EU. These principles are not incompatible with current U.S. structures for protecting health information, such as HIPAA, however, they are in many instances more restrictive and would require additional steps be taken in compliance therewith.

GDPR Applicability to U.S. Health Care Providers

Impact on Health Care Delivery

Health care providers which are solely U.S. based entities will need to determine whether and to what extent they may:

- Offer goods and services to an ***individual located within the EU***; or
- Monitor the behavior of individuals ***located within the EU*** (i.e., monitoring IP traffic, cookies, etc. through a website).

Isolated and infrequent services provided to individuals within the EU or monitoring of behavior *which are not targeted or directed to EU individuals* present a low risk of applicability and enforcement under the GDPR. Activities listed below would present a low risk of applicability and enforcement, unless the provider has targeted or directed services to patient populations in the EU (i.e., representations that provider excels in continuity of care in the international context, care coordinators specifically designated for EU patients, application for use of a patient portal designed specifically for access within the EU).

- Initial information received from a patient while still in the EU but related to a U.S. visit (i.e., appointment request to schedule a U.S. visit, receiving patient health information to determine whether to accept the individual as a patient for the U.S.), and any initial information collected from a patient in order to schedule that appointment, including patient's demographics, insurance information, and any pertinent clinical information collected at that time (whether through a patient portal, messaging or emails);

- Post-discharge communications where the purpose would simply be to identify how the patient is doing (i.e., a general courtesy follow-up verbal call or email, and notation made that a call or email was sent), or general patient satisfaction/perception surveys, or anonymous surveys and data collection processes;
- Form submissions (i.e., submitting an authorization form for copies of his or her medical record to be sent to a UK provider, a request for amendment or restrictions on use of health information, or a request for an accounting of disclosures).

However, the following post-discharge or other health care related activities could be more likely to trigger the GDPR as "offering services" (or potentially also "***monitoring behavior***") if conducted by a provider after the patient has returned home to the EU, particularly where the provider is targeting or customizing the services to EU populations. Isolated and infrequent instances related to the care received while in the U.S., however, *should* still present a low risk of GDPR applicability and enforcement.

1. **Telehealth consults or any other billable health care service** (i.e., follow-ups which would be reimbursable, even if a claim is ultimately not submitted or payment received by the provider) **provided once the individual has returned home to the EU or is otherwise located within the EU.**

2. **Post-discharge surveys and other post-discharge processes** where the provider seeks to analyze, treat and/or monitor additional clinical or behavioral information about the individual once the individual has returned to the EU. This could be viewed as the continued provision of health care services to the individual after the person returns to the EU (as well as potentially the "monitoring" of such individual's health behavior.[5]
   - Where a provider has a higher incidence of patients originating from the EU, workflows should be examined to determine whether post-discharge processes could accommodate a workflow where individuals from the EU do not receive certain post-discharge follow-up, if clinically appropriate.
   - The provider should work with the individual to transfer information to an EU-based provider that will resume or take over care of the individual when s/he returns to the EU.
   - If the workflow cannot accommodate this prior to the data collection, in the alternative, a process could be implemented where EU responses which may be received as part of a general data analytics pool are filtered and not retained, further analyzed or processed.

[5] With respect to monitoring, the following is noted by the European Parliament and Council in the context of the GDPR. "The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. In 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." This appears to govern primarily monitoring of internet-based behavior and actions.

- If follow-up care is clinically required in accordance with acceptable medical standards and the individual cannot be transferred to a EU provider, the provider should avoid targeting the services to EU individuals (i.e. marketing itself out as continuing to provide care to EU individuals when they return home, designating or tailoring care coordination to those individuals within the EU), as well as initiating any new services for the EU individual while located within the EU (i.e., telehealth consults).

3. **Research clinical trials**, where the provider actively recruits EU participants or otherwise may be processing data of EU individuals in connection with an international multi-site clinical trial.

4. **Patient a patient portals**, but only with respect to certain actions, where driven by the provider and targeted toward EU individuals.

   - General use of a patient a patient portal/PHR generally may be likened to use of a general website. If the provider is not specifically holding out the a patient portal to EU individuals (i.e., specifically marketing to or otherwise holding out to EU individuals use of the a patient portal as a convenient way of accessing their US health information, creating a **custom log-in website or application** for a patient portal access in EU geographic regions), this would likely not trigger the GDPR and be viewed as offering a "service" to an individual within the EU.[6]

   - Simply being able to log into and view a patient portal account from the EU (non-customized or targeted), or use an API or other function to transmit information from a U.S. a patient portal account to an EU or other provider, is not likely enough to trigger the GDPR. However, if the provider utilized a **custom log-in created for patients located in a specific country** (i.e., website accessible for Belgium and translated from English), then this customization and targeting of the a patient portal would likely trigger the GDPR.

   - **Collection of any online identifiers** while the individual is logged into the **a patient portal** would also trigger the GDPR (i.e., cookies to manage identity during browser sessions). However, any processing in this manner would likely trigger the GDPR **with respect to the a patient portal vendor only** as the data controller (i.e., the entity determining the means and purposes for which such online identifiers were collected and used), and not with respect to the provider, ***unless*** the provider were engaged in the collection and use of any such identifiers (i.e., would subsequently collect and use the data from the vendor to analyze a patient portal usage by patients across EU regions in efforts to increase utilization).

[6] One could take a position that the "Service" is a patient portal/PHR offering itself, through website browser and/or mobile application, which availability and use within the EU by an individual is sufficient to trigger the GDPR. At this time, there is insufficient guidance to interpret a patient portal/PHR offering this broadly for purposes of the GDPR. To the extent subsequent guidance may be issued related to the "offering of services" by entities outside of the EU, a patient portal/PHR use by EU individuals can be re-analyzed. If a patient portal is only being actively held out to US patients, and is not marketed or otherwise marketed specifically by the provider to individuals in EU regions, then a should not be found to be engaged in offering the patient portal/PHR to EU individuals, even if an individual who receives care in the US and returns home happens to active and use a patient portal/PHR for purposes related to that previously performed US care.

- Using a **messaging system** to ask a general question of the provider's staff, or receiving pre-registration materials to fill out in advance of a visit would not likely be enough to trigger the GDPR. The ability to correct or upload limited demographic and insurance information through a a patient portal would also not likely be viewed as triggering the GDPR where it related to the care provided within the U.S.

- **A a patient portal/PHR** which permits a patient to **upload information** related to care from other providers, or otherwise self-enter medical and other information (e.g., fitness data, etc) ***could*** trigger the GDPR with respect to any subsequent active analyses or monitoring of that data by that provider (i.e., provider requests the information be entered and transmitted by the patient in order to continue the provision of care to the individual). Likewise, integration of "virtual visits" or similar telehealth consultations through a a patient portal/PHR or use of messaging to specifically obtain and analyze additional information from a patient could also trigger the GDPR with respect to such visit and information maintained thereafter.

5. **General Website Use.** The other primary area in which a provider located within the United States could potentially be subject to the GDPR is with respect to website availability, including "monitor[ing] the behavior of individuals located within the EU." The provider will need to identify any data which may be collected/analyzed either directly or through a vendor from the provider's general website (i.e., cookies and browser tracking, whether or not correlated with eventual receipt of services, "contact us" boxes), and whether, to its knowledge, there is website accessibility from within the EU, including with respect to a patient a patient portal/PHR functionality (i.e., no geo-restrictions).

   - Although many U.S. based websites may not be available to view in other countries, simply having a website which could be viewed by an EU resident from within the EU is not enough to be deemed offering services to an individual within the EU triggering the GDPR or monitoring behavior. Use of a general "contact us" box, whereby an individual could fill out for more information about a provider's services, would also likely not be deemed offering services to an individual within the EU or monitoring behavior, because again, the provider is not holding itself out as offering services to those within the EU.

   - However, use of a "Contact Us" box submission by an individual within the EU whose information is *then* analyzed by the provider to correspond to whether the individual actually received care from the provider or analyzed for other purposes to determine how effective the website is, *could* possibly trigger the GDPR as "monitoring" of an individual's behavior within the EU. Any website data analytics conducted by a vendor on behalf of a U.S. provider should generally exclude analyses of non-U.S. contact information where feasible.

   - Likewise, actively translating the website into the language for that EU region, or using the website to hold the provider out as providing care to EU residents from a particular EU region, would likely be viewed as "offering services" within the EU.

However, a hospital that simply arranges for interpreter services for individuals who call or have a treatment visit would not likely be viewed as offering services by virtue of those interpreter services.

- Collection and use of online identifiers (i.e., IP addresses, cookies and geotags), for example, to determine geographic locations from which site visits to the provider's website occurred would also likely trigger "monitoring of behavior" and therefore the GDPR when these functions were performed by or for the provider and related to EU residents. Workflows should be implemented where possible with vendors providing these web-based services to *disable* these functions in EU geographic regions or filter out IP addresses originating from the EU to minimize this risk.

Enforcement of the GDPR

The GDPR attempts to sweep broadly across national borders in order to accomplish its data protection principles for individuals in the EU. For U.S. providers which have no establishment within the EU, and their only contact with a patient results from where a patient has sought treatment within the U.S. originally, questions remain as to whether and to what extent the GDPR will be enforced, even if activities would presume to fall within its scope. Additionally, the GDPR is more stringent in terms of how personal data may be processed, and could additionally result in a U.S. company faced with conflict between those U.S. laws it is obligated to comply with (i.e., U.S. discovery obligations), and its GDPR obligations.

For entities which are not established within the EU or which have not designated a representative within the EU for purposes of the GDPR, **it is not clear how the GDPR would be *enforced*, particularly for U.S. health care providers with limited treatment of EU patients**. Any enforcement action would likely need to occur through the application of international law and cooperation between the U.S, the EU, and EU Member States. The U.S. has not taken any steps at this point to affirmatively implement or enforce the GDPR broadly with respect to U.S. companies except in relation to its commitments under the EU-U.S. Privacy Shield.

The Privacy Shield Framework is one of the limited transfer mechanism available for entities to transfer personal data from the EU to an entity located within the U.S. The Privacy Shield Framework was approved in relation to the predecessor of the GDPR, and therefore, will likely be subject to further amendment under the GDPR. Entities that voluntarily self-certify to the Privacy Shield Framework agree to implement certain data protections and provide certain rights to EU data subjects, as well as submit to the authority of the FTC.

The FTC enforces the Privacy Shield, as may the Department of Transportation and other statutory entities which may be recognized in the future. Notably, any questions related to interpretation or compliance with the Privacy Shield principles are to be resolved through the application of U.S. Law. **However, there is no mechanism for enforcement of the GDPR within the U.S. in relation to entities that have not self-certified to the Privacy Shield.** If an entity has not self-certified to the Privacy Shield, *it would not be obligated to comply with its requirements*. Therefore, where an entity has not self-certified to the Privacy Shield, the entity would need to look to whether the GDPR could be enforced against it either contractually or through another jurisdictional basis, such as by an EU Member State.

Enforcement of any fines or other sanctions which may be sought by an EU data protection authority, Member State or European Commission would likely be subject to review and enforcement by U.S. courts. Although U.S. courts may be more willing to enforce a contractual commitment regarding compliance with the GDPR in terms of agreements between controllers and processors (i.e., a U.S.-based processor that breached its contractual commitments to an EU based controller), it is unclear to what extent they would be willing to enforce international law. There is also the potential for a provider to be potentially sued in the courts of an EU Member State by an aggrieved data subject (i.e., a data breach) or the EU or Member State attempting to exercise jurisdiction, although there would likely be jurisdictional challenges related to any such attempts. Ultimately, for a health care provider that does not actively target or market to EU patients, and only treats such patients infrequently, the risk of direct enforcement for non-compliance with the GDPR, even should limited activities of the provider fall within the scope of GDPR applicability*, is likely low at this time*.

Health care providers, however, will need to take care in any contractual arrangements that they do not contractually agree to comply with the GDPR where such would not likely be applicable to their activities. For vendors which would conduct activities that would render the vendor a data processor for purposes of the GDPR, to the extent that any of their customers would be subject to the GDPR as data controllers (or data processors), they may seek to broadly require that all of their customers agree to comply with the GDPR out of an abundance of caution and their inability to identify customers which may provide services within the EU. Contractual agreements to comply with GDPR requirements (even where such may not apply directly to the provider) could be enforceable by a U.S. court under those circumstances in the event of a breach of contract (i.e., failure to report a breach, failure to implement appropriate safeguards).

* * * *

For more information, please contact:

Krystyna Monticello, Esq.
Partner at Oscislawski LLC
tel: 609-385-0833, ext. 2
kmonticello@oscislaw.com

OR

Helen Oscislawski, Esq.
Principal at Oscislawski LLC
tel: 609-385-0833, ext. 1
helen@oscislaw.com

Attorneys at Oscislawski LLC is a health law firm with its main office located in Princeton, New Jersey but a nationwide reputation for experience with and understanding of federal and state privacy and security laws, as well as electronic health information exchange, health information technology, and managing health data breaches. Our attorneys also advise clients on wide-range of other legal issues. For more information about our firm visit www.oscislaw.com. ***For excellent compliance information, tools and solutions, please also visit our affiliated blog & resource website*** *www.legalhie.com.*