Data protection challenges for telemedicine in the EU and US

Alexis Gilroy, Cristiana Spontoni, Katherine Llewellyn and Undine von Diemar of Jones Day in this article review the regulatory situation for telemedicine and data protection in the EU and US, and the challenges arising for telemedicine providers in both jurisdictions.

Telemedicine, which includes for example teleconsultations, telemonitoring, telesurgery or teleradiology, typically involves the management of delicate/confidential information that is protected under the laws of many countries around the world. Any operator interested in offering services or applications in this space has therefore the thankless task of mapping the applicable requirements, often a titanic endeavour in itself, and then devising and implementing a robust compliance infrastructure.

Telemedicine in the EU

Telemedicine services typically involve the processing of patient health information, where by 'processing' basically any activity that touches the data is covered: from collection to recording, from organisation to storage, from consultation to use or disclosure, and even erasure or destruction[1]. And it's not just written data: personal data also includes sound and image data[2]. While the EU protects (and therefore regulates the processing of) all personal data, patient health information is regarded as 'sensitive' and therefore subject to increased scrutiny and protection. The main vehicle of the applicable rules is Directive 95/46/EC (the 'DP Directive') and its national implementing legislation as adopted in each of the 28 Member States ('MS').

Article 8 of the DP Directive prohibits as a general principle the processing of personal data related to health[3] unless certain conditions are fulfilled. These conditions include to obtain the explicit consent of the person to whom the data belongs (the 'data subject'), or to process the data when necessary to protect the 'vital interests' of the data subject or where processing is required for the purposes of preventative medicine, medical diagnosis, the provision of care of treatment or the management of healthcare services and performed by healthcare professionals who are subject to confidentiality obligations.

Assuming processing is permitted under the mentioned conditions, there are a number of additional obligations that a telemedicine provider must comply with. First of all, health information may only be collected for specific, explicit and legitimate purposes and may not be kept for longer than necessary. This means that 'blanket' consent clauses allowing unspecified uses of the data are typically deemed invalid. Also, patients must be given information regarding the identity of the entity in control of their data (the 'data controller'), of the potential recipients of such data, as well as of any transfer of their data outside of the EU and the existence of their right to access, and rectify, their data. How is that implemented in practice? Robust consent clauses are a very good starting point, and generally data protection authorities around the EU allow consent to be given through electronic means. In this respect, what is key for a telemedicine provider is to be able to maintain an appropriate record/evidence of the consents given.

Moreover, telemedicine operators are expected to implement appropriate technical and organisational measures to protect health data from accidental or unlawful destruction or unauthorised disclosure. No particularly prescriptive rules have been developed in this regard, and it is therefore the responsibility of operators to ensure they are applying state-of-the-art technologies to adequately protect the data they handle.

And then there is the infamous problem of international transfers, which is particularly acute in telemedicine applications given that these often rely on sophisticated communications infrastructure allowing the data to 'travel' around the world: as a general rule, health data may be transferred to third countries outside the EU only if such countries guarantee an 'adequate' level of protection. Where a non-EU country is not deemed to ensure an adequate level of protection (as is the case with the US), the transfer of such data is only allowed under limited conditions. Such conditions include the use of data transfer contracts executed by the EU exporter of data and the receiving parties located outside the EU[4], obtaining the unambiguous consent of the patient, or certification under national rules such as those applicable in the US under the so-called 'Safe Harbor' scheme.

But there is more: processing of personal data may require national filings with national data privacy authorities, even when performed remotely. This is one of the aspects where rules across EU countries differ the most, despite the EU harmonisation that has taken place through the adoption of the DP Directive. So, enough for a pretty challenging puzzle of rules…

Two additional aspects need to be taken into account. First, EU data privacy rules today put the bulk of the compliance burden on the so-

called 'data controllers,' which are those entities that define the 'purposes and means' of a given data processing activity, as opposed to 'data processors,' which are (typically service providers) processing personal data on behalf of controllers. This is a very important distinction in the world of telemedicine as oftentimes telemedicine providers are simply acting on the instructions of third parties such as insurers, health organisations, doctors associations, etc. While a case-by-case analysis needs to be carried out in each of these circumstances, and oftentimes it is tricky to define roles in a telemedicine environment, many service providers can potentially just qualify as processors and therefore be 'off-the-hook' as regards many of the compliance obligations imposed by the current EU rules.

Second, change is upon us: in January 2012, the European Commission ('EC') proposed new rules aiming at ironing out national divergences and providing a single set of rules directly applicable across the MS[5]. In the words of the EC, the proposed regulation will "facilitate the cross border exchange of health data while preserving a high level of protection."[6]

In addition to increasingly uniform rules, the proposed Regulation foresees various new concepts not currently included in the DP Directive. For example, and of relevance to telemedicine operators, are: the right for the patient to be forgotten, i.e. the right of a patient to get their data erased; and a right on data portability at patients' request, i.e. the right for data subjects to transfer their personal data in a commonly-used electronic format from one data controller to another without hindrance from the original controller.

Many telemedicine service providers can potentially just qualify as processors and therefore be 'off-the-hook' as regards many of the compliance obligations imposed by the current EU rules

Furthermore, it is proposed that the new rules will apply to entities established outside the EU whenever they process personal data, in connection with the provision of services or monitoring of EU citizens. This is a significant change compared to the existing rules, which in general apply only to processing of personal data (directly or through delegates, i.e. the 'processors' referred to earlier in this article) in the EU.

An issue of hot debate under the proposed Regulation is whether the further processing of health data for scientific research purposes should be permitted only with the consent of the data subject and if certain safeguards for individuals' rights and freedoms are met, or whether it should be admissible without consent, provided said safeguards are met[7]. While the EC and the Council favour the approach of not requiring consent, the Parliament insists on consent.

Telemedicine in the US

In comparison to the EU structure for privacy, in the US, telemedicine and telehealth providers face a slightly different challenge when evaluating applicable compliance requirements - namely, which rules apply. A telemedicine provider may be subject to federal government requirements under the Department of Health and Human Services or the Federal Trade Commission ('FTC'), state-specific laws and regulations, or all of the above. Further, vendors to telemedicine providers (both technology IT platform and data storage vendors) can be subject to both direct enforcement by federal regulators and contractual requirements in Business Associate Agreements.

While telemedicine, the practice of medicine albeit through a delivery method whereby a physician is remote from the patient at the time of the encounter and communicating through telecommunications technology, is in theory subject to all of the same privacy and security requirements as traditional methods of delivering healthcare, the business models common for telemedicine in the US and some of the more recent state-specific laws and regulations governing telemedicine often modify traditional application of US privacy and security laws and regulations. The following high level overview highlights some of the unique applications of US privacy and security law as it relates to telemedicine.

The Health Insurance Portability and Accountability Act 1996 ('HIPAA')[8] protects personal health information ('PHI') and was further clarified and expanded, especially as it relates to electronic transfers and communications, in the Health Information Technology for Economic Clinical Health Act 2009 ('HITECH')[9]. The US Department of Health and Human Services ('HHS'), the federal agency with primary authority for overseeing the enforcement of HIPAA and HITECH, has promulgated a variety of rules as to specific privacy and security requirements under both laws, most notably with the 'Omnibus Rule' published in early 2013. Only certain parties, called 'covered entities' and, since the Omnibus Rule, 'business associates,' are subject to HIPAA. 'Covered Entities' include: (i) health plans, (ii) healthcare providers, and (iii) healthcare clearing houses. A 'business associate' is defined as an entity that: (i) creates, receives, maintains, or transmits 'protected health information' to perform certain functions or activities on behalf of a covered entity, (ii) provides legal,

actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to, or for, a covered entity in situations where PHI is involved, (iii) provides data transmission services to a covered entity and has access to PHI on a routine basis, (iv) administers personal health records to one or more individuals on behalf of a covered entity, or (v) operates as a subcontractor of the business associate who has been delegated a function, activity, or service in a capacity other than as a member of the business associate's workforce.

Telemedicine does not alter a covered entity's obligations under HIPAA or HITECH, nor does either statute contain any special section devoted to telemedicine. In short, if a covered entity exchanges PHI in the course of the telemedicine encounter, the covered entity (and its business associate) must meet the same HIPAA and HITECH requirements that it would for a service provided in-person[10]. Interestingly, as only limited telemedicine services are reimbursed by Medicare[11] and Medicaid[12], some telemedicine healthcare providers are not participating in any federal healthcare payor programs and thus may not be technically subject to some or all of the requirements of HIPAA or HITECH under the federal statutes and rules. In such circumstances, the telemedicine provider would be subject to the FTC's more general requirements regarding use of consumer information and data[13].

Further, state privacy, consumer protection, and telemedicine laws may also be applicable to telemedicine providers whether or not HIPAA or HITECH applies. Where HIPAA applies to the telemedicine provider, state laws that are more stringent than HIPAA also apply, although HIPAA supersedes state laws with lesser requirements than HIPAA. Additionally, certain states have recently adopted telemedicine specific statutes or rules that contain requirements applicable to telemedicine providers that are more specific or stringent than HIPAA and, in some cases, require compliance with HIPAA even where a provider is not otherwise subject to HIPAA[14]. As such, a telemedicine provider who does not participate in a federal healthcare program or receive any PHI may still be required to comply with HIPAA and more stringent privacy practice and notice requirements for the purposes of meeting state requirements.

Conclusion

Entrepreneurs are continuing to develop interfaces and mobile medical applications for virtual physician-patient and physician-physician interactions, and the related business models will continue to evolve. Prior to utilising these telemedicine technologies, providers should understand how they collect and transfer patients' health information, ensure that they have secure communication channels, and implement appropriate documents, educate administrators and users regarding the appropriate use of telemedicine technologies, and understand how and what patient information is being collected and stored. This is a thankless - but not impossible - task, particularly if managed in a proactive manner, ideally at the design phase of the related telemedicine applications.

Alexis Gilroy Partner
Cristiana Spontoni Partner
Katherine Llewellyn Associate
Undine von Diemar Partner
Jones Day, Washington DC, Brussels and Munich
agilroy@jonesday.com
cspontoni@jonesday.com
kllewellyn@jonesday.com
uvondiemar@jonesday.com

1. See Article 2(b) of the DP Directive.
2. See the EC's Working Document on the Applicability of the Existing EU Legal Framework to Telemedicine Services (SWD (2012) 414 final).
3. According to the European Court of Justice (see Case C-101/01), the notion of 'data concerning health' must be given a wide interpretation, so as to include information concerning all aspects, both physical and mental, of an individual's health.
4. In this regard, the EC has proposed standard contractual clauses that ensure an adequate level of protection of transferred personal data.
5. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012) 11 final).
6. See the EC's Working Document on the Applicability of the Existing EU Legal Framework to Telemedicine Services (SWD (2012) 414 final), at section 3.2.2.
7. See the conditions mentioned in Art. 83 of the Regulation.
8. Pub. L. No. 104-191, enacted 21 August 1996.
9. Pub. L. No. 111-5.
10. Use of specific telehealth equipment or technology cannot ensure that an entity is 'HIPAA-compliant,' because HIPAA addresses more than features or technical specifications.
11. Medicare coverage for telemedicine is limited to real-time video and audio services provided by certain types of practitioners for only specific medical services where the patient is in a particular type of health facility located in a rural area. See http://www.americantelemed.org/docs/default-source/policy/medicare-payment-of-telemedicine-and-telehealth-services.pdf?sfvrsn=14
12. Coverage for telemedicine under the Medicaid program is based on state-by-state rules with only minimal reimbursement coverage in some states. See http://www.americantelemed.org/docs/default-source/policy/50-state-telemedicine-gaps-analysis---coverage-and-reimbursement.pdf?sfvrsn=10
13. https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy
14. See Title 46 Louisiana Professional Occupations Standards Chapter 75, Section 7510.