Digital health: legal challenges in the European Union

Blanca Escribano
IBA Communications Law Committee Secretary; CMS Spain, Madrid
blanca.escribano@cms-asl.com

Digitalisation and the fourth industrial revolution is especially impacting the health ecosystem. Technologies like the Internet of Things (sensors), virtual reality, 3D printing, robots, machine learning algorithms, mobile communications, web portals, social media, big data analytics and patient engagement platforms are shaping a new reality called digital health, e-health or m-health, depending on the level of technology support. Tech companies are entering the health ecosystem and in the very near future, most drugs will have both a chemical and digital component. That is why the industry is identifying data as 'the new drug'.

Legal challenges like access, ownership, portability and free movement of data are being tackled at European Union level and addressed here.

Market and trends

We are currently seeing the tip of the digitalisation process iceberg, starting what some people call 'the fourth industrial revolution'. The digitalisation of the economy means that industrial sectors are not only implementing new technologies in their processes but transforming the entire value chain. Traditional industries like the automotive, pharmaceutical and utilities sectors are being accessed by tech giants that are becoming new players and challenging the status quo. Digital innovations (especially information and communication technologies and data analytics) are converging with the elements and decision-making structures of traditional value chains.

However, the digitalisation process in which every industry is currently immersed is especially affecting the health ecosystem. Healthcare providers are seeing these technological changes as an opportunity to reduce costs and achieve better patient outcomes. Payers (as national health systems) or insurers are obviously interested in implementing these new technologies to reduce some of the fixed infrastructure costs that are necessary to provide onsite attention and increase the effectiveness of drugs by monitoring how they are consumed and their outcomes on the different groups of patients. In addition to the improvements that it may have in developed markets, where this can have a disruptive effect, is in undeveloped countries where not everyone has access to medicine. Digital health could mean the extension of the scope of reach of medicine and access to medicine to groups of people that were excluded from health services or had them available, but in very precarious conditions.

Web portals and telemedicine[1] are enabling direct channels of communication between manufacturers and patients to help understand usage habits, support the exchange of results in medical trials, save costs, increase revenues and, mostly, improve relationships with doctors and enable remote diagnosis (e-health).

With the proliferation of smart handsets, apps that help patients in achieving the best use of pharmaceutical products and treatments are improving outcomes (m-health).[2]

Nevertheless, it will be the industrial Internet of Things (IoT) that will take healthcare to the next level. The use of wearables, body sensors and the most disruptive development, the so-called 'chip in a pill',[3] will make this industry a truly 4.0 one, boosting the full digital health value chain.

The most important way technology is improving and will improve the healthcare industry by making it more predictive is by using more and more precise and sophisticated data. The gathering of – even inside body – data and the use of complex big data analytics (ie, the IBM Watson Health platform) is putting the health industry at a different level. Machine learning backend

means the more data that is fed into the system, the better our understanding will be of which therapies are effective on, for instance, mutations of cancer.

It is being said that, really, what can conquer cancer is data .[4] However, for data-driven medicine and before algorithms, machine learning and big data can be leveraged, it is necessary to connect and pool data in, at least (if not single), interoperable systems, as well as the sharing of information and free flow of data. The idea of collective and non-proprietary clouds, or at least interoperable and interconnected databases for the exchange of (anonymised) health data, is something that could boost research and treatment therapies.

In the very near future, most drugs will have both a chemical and digital component, as every pill will have an accompanying mobile app that collects patient-specific data. We are entering an era in which data will be as important as the drug itself in the therapeutic management of the patient. Unlike traditional passive therapies, the data will enable therapeutic recommendations that are tailored to the individual and actionable. Hence, data is the new drug, as widely acclaimed in this sector.

New business models are being developed to 'beyond the pill'[5] models. Companies are evolving from the sole sale of drugs to the provision of services: pharma as a service in order to embrace a more personalised approach that incorporates acquiring mobile data, medical devices, health IT, big data and the Internet of Everything.

Under this new reality, healthcare companies are facing new competitors from the tech industry. Tech giants such as Google, Apple, Qualcomm and Microsoft are investing heavily in HealthTech. For instance, and as an interesting example of what tech can do for healthcare, in 2015, Google filed a patent application with the World Intellectual Property Organization (WIPO) for a wrist-worn device that could destroy cancer cells in the blood. The patent application, which has the name 'Nanoparticle Phoresis', describes a wearable device that 'can automatically modify or destroy one or more targets in the blood that have an adverse effect on health'. As result of this evolution, partnerships between life sciences companies and tech giants are increasing, combining expertise to bring innovative therapies to the market.

Finally, and from a patient point of view, it is not just physicians making judgments, but patients who are empowered with their own data and who control, own and manage it to make their health decisions. Patient empowerment is boosted by tools like data portability.

Legal challenges and the European Union approach

The European Commission is determined to achieve a Digital Single Market that will replicate the physical single market in the digital ecosystem. The final purpose is 'to achieve an inclusive digital society which benefits from the digital single market: building smarter cities, improving access to e-government, e-health services and digital skills will enable a truly digital European society'.

Starting from the eHealth action plans, the first launched back in 2004 and the second in 2011,[6] European regulators have tackled the legal issues that arise from the provision of health services by digital channels.

Having set the scene, now for a few words on the regulatory and legal challenges. The healthcare sector is highly regulated, regardless of whether operating in the physical field or using digital channels. European regulators have been tackling the legal challenges since the aforementioned eHealth plans were published. To name a few instruments, the Art29WP Opinion on the processing of personal data relating to health in electronic health records (2007),[7] the mHealth Green Paper (2014)[8] and the Staff Working Document on the existing EU legal framework applicable to lifestyle and well-being apps,[9] the EDPS Opinion on mHealth (2015)[10] and the Code of conduct for mHealth apps (2016).[11]

In addition, there are some other non-sector specific opinions and regulations that apply because of the use of digital means, for instance, the Art29WP Opinions on apps on smart devices (2013)[12] and on the IoT (2014),[13] and the ePrivacy Directive, which is currently under review in the form of a Regulation.[14]

Some of the main legal issues that must be considered when dealing with digital health products or services are: (i) whether the app or the software qualifies as a medical device and therefore is subject to the sector-specific strict obligations;[15] (ii) whether it is a lifestyle and wellness or purely a health product or service;[16] (iii) security; (iv) liability across the complex value chain[17] for any damages

resulting from a (software, connectivity, machine) fault in a connecting device;[18] and (v) interoperability and standards.

However, as described above, what is disrupting the health sector is what technology is doing to provide access to patients' data (machine-generated or not) and how treatments interact with them.

When data relates to identifiable individuals and has not been made fully anonymous, it is personal data. In the EU, personal data is regulated by the General Data Protection Regulation (GDPR),[19] a horizontal legislation that applies to all sectors, and the ePrivacy Directive that concerns the confidentiality of electronic (including Over the Top) services (*lex specialis*) and which aims to ensure a high level of protection in full coherence with the GDPR. Health data[20] is treated by the GDPR as a 'special category' of personal data which is considered to be sensitive by nature. Processing is prohibited unless exceptions apply, such as the provision of the individual's explicit consent; it is necessary for achieving purposes in the public interest, for scientific or historical research purposes or statistical purposes; or where Member States have inserted further conditions or limitations. Both the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including pseudonymisation and the encryption of personal data. In summary, health data must comply with higher protection and security standards.

When data is non-personal (or has been anonymised), GDPR and ePrivacy do not apply. The European Commission, with the purpose of achieving a true single digital market, has published the 'Building a European Data Economy Communication'[21] which intends to tackle restrictions on the free movement of data for reasons other than protecting personal data and in order to enable the market players to extract value from all kinds of data by creating a variety of applications, including remote healthcare.[22]

The issue of access to machine-generated data is under consideration in several sectors including healthcare. In some circumstances, producers of raw machine-generated data are protected by the Data Base Directive,[23] also under review at present, and the Trade Secrets Protection Directive.[24] Data ownership across the value chain and voluntary data sharing is something that the different parties involved should regulate in their commercial agreements to fill the gaps in the regulatory framework.

Data portability is a key issue in the data economy, whether it is personal or not. It means that consumers and businesses can easily take their data from one system to another to reduce the switching costs and entry barriers. In the digital health sector, the common use of this right is widely expected. While GDPR introduces the right to personal data portability for data subjects and service providers, there is no legal obligation to port non-personal data (ie, by cloud hosting providers). Consequently, the European Commission is considering developing standard contract terms requiring service providers to implement portability and extending those rights to non-personal data, in particular to cover business to business contexts.

Data portability is closely related to interoperability and technical standards. The EU Commission is also considering launching sector-specific experiments on standards involving industry, technical community and public authorities.

Finally, security in the healthcare industry is critical and, as such, there are different mandatory security obligations in a diverse legal framework. Not only do the GDPR security obligations apply, but also the critical infrastructures[25] and security of network and information systems regulations.[26] Ransomware attacks to hospitals, both in Los Angeles in February 2016 and more recently in the UK in May 2017, evidence the risks that this sector is facing.

To conclude, it would not be an overstatement to say that the application of next generation technology and the entry of tech players into the health market will mean a change of paradigm comparable to that which penicillin entailed a century ago. No doubt, healthtech will benefit the full ecosystem, patients and also stakeholders as the market will significantly grow and there will be more services demanded across the value chain. Blockchain technologies for granting better security and control of data needs may play an important role as the market evolves, but this is another story for another time.

Notes

1 Telemedicine services: interaction between doctors and patients through electronic media.

2 According to the European Commission, mHealth is a sub-segment of eHealth and covers medical and public health practice supported by mobile devices. It especially includes the use of mobile communication devices for health and well-being services and information purposes, as well as mobile health applications.

3 Consumption captures health status, including drug effects on key organs, and sends to a wearable device. The data is then sent as a report over the cloud for diagnosis.
4 Peter Piot, *Wired Health* 2017.
5 Michelle Longmire MD, a Stanford-trained physician-entrepreneur and Chief Executive Officer of Medable.
6 One of the instruments on which the Commission is relying on is the eHealth second action plan 2012–2020 (Brussels, 6.12.2012 COM(2012) 736 final Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions eHealth action plan 2012–2020 – innovative healthcare for the 21st Century), and the Accompanying document Commission Staff Working document on the applicability of the existing EU legal framework to telemedicine services (Brussels, 6.12.2012 SWD(2012) 414 final).
7 'Article 29 Data Protection Working Party', Working Document on the processing of personal data relating to health in electronic health records (HER).
8 Green Paper on mobile Health ('mHealth') SWD (2014) 135 final (Brussels 10.04.2014 Com(2014) 219 final).
9 Commission Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps – Accompanying the document Green Paper on Mobile Health ('mHealth') COM(2014) 219 final (Brussels, 10.4.2014 – SWD(2014) 135 final).
10 European Data Protection Supervisor Opinion 1/2015 Mobile Health 'Reconciling technological innovation with data protection', 21 May 2015.
11 The Code of Conduct on privacy for mobile health apps was formally submitted for comments to the Article 29 Data Protection Working Party in June 2016. Once approved by this independent EU advisory group, the Code will be applied in practice: app developers will be able to voluntarily commit to follow its rules, which are based on EU data protection legislation.
12 Article 29 Data Protection Working Party Opinion 02/2013 on apps on smart devices, adopted on 27 February 2013 (00461/13/EN – WP 202).
13 Article 29 Data Protection Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things, adopted on 16 September 2014 (14/EN - WP 223).
14 Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (Brussels, 10.1.2017 COM (2017) 10 final 2017/0003 (COD)).
15 Guidelines on the qualification and classification of standalone software used in healthcare within the regulatory framework of medical devices. Ref Ares (2016) 3473012 – 15/07/2016. Qualification criteria as a medical device are the following: is it a standalone software or an accessory to the medical device?; does the software perform an action on data?; is it designed to monitor individual patient's data?; and is it designed to be used as a health product?
16 This distinction is not always easy but is important because the Consumer Directive applies to lifestyle and wellness products but not to health ones, which are excluded from the scope thereof and regulated by sector specific rules.
17 Complex interdependencies between different layers as, for instance and at least, the connectivity provider and the internet service provider, the healthcare practitioner, device manufacturer and distributor, app distributor, app developer, the patient/user.
18 The EU Commission has launched a broad evaluation of the Products Liability Directive to assess its overall functioning and whether its rules need to be adapted to emerging technologies such as the IoT and autonomous connected systems. Intermediary liability rules (app store and marketplace as hosting service providers?) must also be considered.
19 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 (General Data Protection Regulation).
20 'Data concerning health' is defined for the first time under EU Data protection law as 'personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status'.
21 'Building a European Data Economy' (Brussels 10.1.2017 COM (2017) 9 final). Commission Staff Working Document on the free flow of data and emerging issues of the European data economy – Accompanying document Communication 'Building a European Data Economy' (Brussels, 10.1.2017 – SWD(2017) 2 final).
22 By the end of 2017, the Commission will present an initiative to abolish unnecessary barriers on where data is located.
23 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.
24 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, to be transposed into national law by June 2018.
25 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection; Commission Staff Working Document on the review of the European Programme for Critical Infrastructure Protection (EPCIP) (Brussels, 22.6.2012 - SWD(2012) 190 final); Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection 'Making European Critical Infrastructures more secure' (Brussels, 28.8.2013 – SWD(2013) 318 final).
26 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.