The emergence of integrated health information systems, mobile apps and software-based medical devices presents significant opportunities for diagnosing illnesses, engaging in preventative medicine, managing healthcare costs and achieving better outcomes. This technological innovation has given rise to new legal, regulatory and commercial challenges.

Many companies are developing integrated, software-based applications to optimise traditional medical devices. In May 2008, a European Commission (Commission) consultation on medical devices was launched. As a result, medical device manufacturers have developed and are in the process of developing wireless-enabled medical devices and mobile apps that allow healthcare providers to access and evaluate patient vital signs and other information through remote monitoring or cloud-based data-sharing systems. The telecommunications industry, software developers and Internet service providers are also providing wireless solutions, technical support and healthcare solutions to healthcare providers, consumers and health systems.

Among other things, this has raised questions in relation to:

- The regulation of these products as medical devices.
- Privacy and movement of personal information.

DEFINITIONS AND EU APPROACH TO REGULATION

Background to EU policy on eHealth and mHealth

Enabling technologies are important for the prevention of illness and improvement and timely delivery of treatment, particularly:

- eHealth (the use of information and communication technologies (ICT) for the provision of health-related services).
- mHealth (the use of mobile communication systems for the provision of health-related services).
- Genomics (the use of a genetic blueprint to identify patient response to treatment or patient susceptibility to a clinical condition or disease. Such information may be presented in an electronic format as a “gene chip”).

The Commission has published several communications on technology and the provision of health products and services. These include:


The impact of information technology (IT) on cross-border healthcare provisions was recognised by the Commission in its policy paper published in 2007, where ICT and allied enabling technologies were considered as particularly important in tackling these new healthcare challenges in the coming decades. Three key challenges were identified by the Commission:

- Demographic changes, including an ageing population.
- Emerging health threats, including new communicable disease patterns resulting from climate change.
- An evolution in healthcare systems, partly due to the rapid development of new technologies, which is revolutionising the promotion of good health and the prediction, prevention and treatment of illness.

Similarly, the European Medicines Agency (EMA) in its “Road Map to 2015 on contributions to science, medicines and health” (see website, http://www.ema.europa.eu/docs/en_GB/document_library/Report/2011/01/WC500101373.pdf) also recognises the impact of new technologies, including eHealth, on existing healthcare systems.

In its assessment on innovation in the medical device sector published in 2011, the Council of Ministers also recognised the need to consider the inter-operability and safety issues related to the integration of medical devices in eHealth systems, especially personal health systems and mHealth systems. However, the deployment of ICT systems is entirely a matter of national competence. Certain industry interest groups or initiatives have been established that have advocated the need for clarity and certainty on regulatory standards to ensure timely market access to emerging IT technologies related to eHealth and mHealth. These include the industry group the European Co-ordination Committee of Radiological, Electromedical and Healthcare-IT Industry (COCIR), which represents many key industry players such as:

- The European Health Telematics Association.
- The European Institute for Health Records.
- Integrating the Healthcare Enterprise.
The "eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century" [see website, http://ec.europa.eu/health/ehealth/docs/com_2012_736_en.pdf] was a communication issued by the Commission on 6 December 2012 directed at issues affecting the increased use of eHealth including:

- Opportunities and benefits.
- Barriers to deployment.
- Inter-operability and EU-wide standards and testing.
- Legal issues including data protection, liability and licensing of professionals.

**Green paper on mHealth**

The Green Paper refers to the World Health Organisation definition of mHealth as covering medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants and other wireless devices. The Green Paper covers software applications and health information and medication reminders delivered to mobile devices.

The application of these technologies to the healthcare field moves the focus more towards preventative medicine and improving patients’ lifestyle. The associated benefits include lowering costs and supporting inter-operability across national boundaries, facilitating patient mobility and safety.

The benefits outlined by the Green Paper include:

- Collection of medical, lifestyle, activity and environmental data for medical practitioners to enable better and more accurate, efficient and personalised treatment.
- Facilitating patients’ access to their medical information and enabling patients to adopt lifestyle changes to engage in preventative medicine and to live more independently.
- Reducing the cost of healthcare and increasing disease prevention.

The e-commerce revolution will have an important enabling role on eHealth and mHealth to ensure high quality, safety and efficient cross-border healthcare provisions within the EU and beyond. In its communication relating to telemedicine (providing healthcare services at a distance), the Commission indicated that eHealth can help improve the lives of EU citizens, both in terms of patients and health professionals. However, as the Commission has put it, integrating healthcare services systems such as tele-radiology (the transmission of radiological patient images, x-rays, CTs, and MRIs, from one location to another) and tele-consultation (consultations where the healthcare provider and the patient are not at the same location) is a challenging task. The main issues concern:

- Building confidence in and acceptance of tele-medicine services.
- Bringing legal clarity, particularly in relation to the relevant regulatory regime.
- Solving technical issues and facilitating market development.

One area of uncertainty is the extent to which lifestyle and fitness apps should be regulated as medical devices or in vitro medical devices. There is no EU legislation delineating the distinction. However, there is some Commission guidance (see website, http://ec.europa.eu/health/medical-devices/files/meddev/2_1_6奧_en.pdf), that focuses on the purposes of the app to determine whether it is a medical device or in-vitrodiagnostic (IVD) medical device.

Certain medical device manufacturers have applied for the European Conformity mark (CE-mark) to be affixed to their patient care network or mobile software, including apps designed to facilitate transmission of patient records for the purposes of diagnosis and choice of treatment, as well as outcome measurements.

More recently, the Commission has started paving the way for an industry-led Code of Conduct for mobile health apps, covering the topics of privacy and security. The aim of the code would be to help key players adhere to the legislative framework governing mobile health apps. This initiative was discussed at an mHealth stakeholder meeting on 12 May 2015. The discussion at the meeting built on the Green Paper on mHealth public consultation results. The need for a Code of conduct was emphasized by the concerns of attendees. These centered on the potential lack of clinical evidence that apps base themselves on and a risk they could be misleading and/or unsafe. Nevertheless, the Commission presented initiatives such as those under the Startup Europe (https://ec.europa.eu/digital-single-market/en/startup-europe) and the Digital Single Market Strategy (http://ec.europa.eu/priorities/digital-single-market/) to support web entrepreneurs’ access to the market. A second stakeholder meeting took place on 6 July 2015 where the Commission continued to discuss facilitating the development of a European standard on quality criteria for health and wellbeing apps. In doing so the stakeholders looked at specification PAS277 recently published by the British Standards Institution. The stakeholders also announced their intention to drum up support for voluntary certification and began looking at how some members states deal with certification.

A working group was formed after a public "call for expression of interest" by the Commission, 20 applications were selected and the group will have its first meeting in March 2016 with guidelines expected to be finalised by the end of 2016.

**EU REGULATION OF MEDICAL DEVICES**

In the EU, medical devices, low voltage equipment, machinery and radio and telecommunications terminal equipment are regulated under the “New Approach” directives, which provide for the affixing of a CE-mark. The New Approach directives are based on Council Resolution of 7 May 1985 on a new approach to technical harmonisation and standards (85/C 136/0). The main EU directives relating to the safety and performance of medical devices are:


These have been supplemented by modifying and implementing directives, including Directive 2007/47/EC amending Directives 90/385/EEC, 93/42/EEC and 98/79/EC (Medical Devices Amendment Directive).

The purpose of these directives is to contribute to the development of the single market. The European standardisation system is designed to remove technical barriers to trade and facilitate free movement of goods between member states.

The New Approach directives set out a new regulatory approach based on the following agreed guiding principles:

- Legislative harmonisation is limited to products placed on the EU market that meet the essential requirements and benefit from free movement within the EU.
- Technical specification for assessing conformity with the essential requirements is set out in harmonised standards.
- Application of harmonised or other standards remains voluntary and the manufacturer can apply other technical specifications to meet the requirements.
• Products manufactured in compliance with harmonised standards benefit from a presumption of conformity with the corresponding essential requirements.

In essence, manufacturers and bodies assessing for conformity with the harmonised standards use the standards to demonstrate compliance with relevant EU legislation.

The New Approach directives require national standards to offer a guaranteed level of protection to the extent of the essential requirements established by the directives. They also require the national authorities to carry out their responsibilities to protect safety or other interests covered by the directives. Under the New Approach directives, a safeguard clause procedure is required to allow for contesting a product’s compliance, or failures or shortcomings of harmonised standards.

The procedure for conformity assessment under the New Approach directives is risk-based, taking account of the classification of the medical device, the intended clinical mode of use and the nature and characteristics of the device. In the EU, medical devices fall into the following four distinct classes according to the risk assessment and characterisation:

• Class I (lowest risk).
• Class IIa.
• Class IIb.
• Class III (highest risk).

This allows for a graduated system of control.

The test for establishing essential requirements seeks to ensure that the device is designed and manufactured in such a way that when used under the conditions and for the purposes intended, it does not compromise clinical conditions or safety. Any risks associated with its intended use should be acceptable risks when weighed against the benefits to the patient. The benefit/risk assessment should be compatible with the overarching objective of achieving a high level of health and safety protection.

Stand-alone medical software and medical software in devices

Under the current rules, devices that incorporate software, or that are medical software in themselves, must be validated according to the state of the art, taking into account the principles of development lifecycle, risk management, validation and verification.

Under EU rules, stand-alone software can be considered an active medical device (that is, any device operation that depends on a source of electrical energy or any source of power other than that directly generated by the human body or gravity, and that acts by converting this energy). Medical devices intended to transmit energy, substances or other elements between an active medical device and the patient without any significant change are not considered to be active medical devices.

Under the amendment to the Medical Devices Directive adopted in 2007 in the Medical Devices Amendment Directive, a medical device can include software either as a stand-alone device or in combination with another device for a medical purpose.

A medical device is now defined in the revised Medical Devices Directive to mean any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, together with any accessories, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for a medical purpose, provided that the principal intended action is not mediated through a biological process.

An assessment of a medical purpose is usually based on the declared claims made by the manufacturer on the label, instructions for use and the promotional material consistent with the overarching purpose of the Medical Devices Directive to ensure a high level of protection for patients and consumers.

The Commission’s established position distinguishes between two types of software:

• Software influencing the proper functioning of a device.
• Software used in combination with non-medical equipment.

Software related to the functioning of a medical device can be regulated as a stand-alone medical device or as an accessory to the medical device under the Medical Devices Directive. Software used with non-medical equipment is not considered a medical device.

The key test is whether the software provides for a proper diagnostic or therapeutic purpose.

If the definition for a medical device, which is sufficiently broad and all encompassing, were to be given its purposive meaning according to established European jurisprudence, equipment, appliances or apparatus involved in eHealth or mHealth could be regulated as a medical device. This classification in itself may be somewhat artificial, given that mobile software equipment and appliances similar to medical devices are in any case regulated under the New Approach directives, which seek to address all hazards or risks to the public interest that the amended Medical Devices Directive intends to protect, such as the protection of consumers, patients or users. According to the Commission, regulatory compliance with the essential requirements can often require simultaneous application of more than one New Approach directive, and possibly other EU legal instruments.

In its public consultation document concerning the recast (codification or consolidation) of the Medical Devices Directive, the Commission asked whether the current approach to assessing essential requirements is sufficiently robust for innovative technologies and practices involved in the development of eHealth or mHealth across the EU, including those based on nanotechnology, genetic testing and advancements in IT. The consultation document also asked whether appropriate adaptation or reinforcement of the established principles underpinning essential requirements is required in the recast of the Medical Devices Directive.

2012 Commission guidance on stand-alone software

In 2012, the Commission published guidance to define the criteria for the qualification of stand-alone software as a medical device (see http://ec.europa.eu/health/medical-devices/files/meddev/2_1_6_el_en.pdf) (Guidelines). The Guidelines are not legally binding, but they are similar to the guidance issued by the US Food and Drug Administration and were prepared in consultation with Competent Bodies, Industry and Notified Bodies. The Guidelines set out the qualification criteria for stand-alone software to be a medical device. The software must have a medical purpose (as described by the manufacturer). The Guidelines also set out that if the stand-alone software does not meet the definition of a medical device or IVD medical device but is intended by the manufacturer to be an accessory to a medical device or an IVD medical device, then the software would be regulated respectively under the Medical Devices Directive or IVD Directive.

The Guidelines contain two decision diagrams, one to aid in determining whether stand-alone software is a medical device, and a second to assist qualification as an IVD medical device.

Stand-alone software as a medical device. An important qualification set out in the Guidelines is that if the software merely performs an action on data, or performs an action limited to storage, archival, communication, “simple” search or lossless compression, it is not a medical device. In addition, embellishing the representation of data does not automatically make the
software a medical device but where the data alters the representation of data for a medical purpose or is intended to create or modify medical information, then it may be a medical device. Three further points are made in the explanation of the decision diagram:

- If such alterations to data representations are made to facilitate the perceptual and/or interpretative tasks performed by the healthcare professionals when reviewing medical information, then it may be a medical device.
- If the manufacturer intends the software to be used for any of the purposes listed in Article 1(2)a of Medical Devices Directive, then it is a medical device. However, tasks such as emailing, web or voice messaging, data parsing, word processing and backing-up are by themselves not considered as having a medical purpose under the Medical Devices Directive.
- Where the software is merely an accessory, then it is not a device, but instead falls under the IVD Directive.

**Stand-alone software as an IVD medical device.** The Guidelines also set out that stand-alone software that fulfills the definition of a medical device falls under the IVD Directive if the following two points are met:

- The stand-alone software is intended to be used for the purpose of providing information derived from in vitro examination of a specimen derived from the human body.
- The manufacturer specifically intends the stand-alone software to be used with an IVD medical device to enable that device to be used in accordance with its intended purpose.

If so, then the software is an IVD medical device under the IVD Directive. However, software that merely collects and transmits information to a centralised database or manages feedback is not an IVD medical device.

**Classification of stand-alone software.** Two principles are stated at the beginning of this section of the Guidelines:

- Stand-alone software that meets the definition of a medical device is considered as an active medical device. This means that rules 9, 10, 10, 11 and 12 of Annex IX to the Medical Devices Directive apply.
- Clause 2.3 of the implementing rules in Annex IX states that software that drives a medical device or influences the use of a device falls automatically into the same class as the device it drives.

The Guidelines list types of software, their classification under Annex IX of the Medical Devices Directive and gives examples as follows:

- Software as active therapeutic devices. These fall under classes Ila or Iib. Examples would be a radiotherapy planning system used to calculate the dose of ionizing radiation to be administered to the patient or insulin dosage planning stand-alone software.
- Active devices intended for diagnosis fall under class Ila if they are intended to image in vivo distribution of radiopharmaceuticals. An example given is the clinical application of registration of PET datasets on CT datasets for follow-up tumour treatment.
- Active devices intended to allow direct diagnosis or monitoring of vital physiological parameters fall under class Ila. An example would be software for the presentation of the heart rate or other physiological parameters during routine check-ups.
- Active devices intended for the monitoring of vital physiological parameters where the nature of variations is such that it could result in immediate danger to the patient fall under class Iib.

**Analysis of examples.** Annex 1 of the Guidelines analyses six types of devices and assesses whether they are qualified as medical devices under the regulatory framework:

- Hospital information services.
- Decision support software.
- Information systems.
- Communication systems.
- Web systems for monitoring of data.
- IVD software, such as laboratory information systems and work areas managers.


The Guidelines set out that the following software examples would be considered medical devices:

- Radiotherapy treatment planning systems intended to calculate the dosage of ionising irradiation to be applied to a patient.
- Chemotherapy planning systems intended to calculate the drug dosage to be administered to a patient.
- Computer-aided detection systems intended to provide information that may suggest or exclude medical conditions such as systems that automatically read x-rays or interpret ECGs.
- Image viewers with functionality for diagnosis based on digital images.

**Standard for conformity assessment of medical software**

Under the New Approach regulatory framework, a medical device is presumed to conform with the essential requirements if it meets the appropriate harmonised standard. It was considered that, until the amendment of the Medical Devices Directive, safety regulations for medical device software, at least formally, were not sufficiently rigorous to the extent that medical software was not legislatively classified as falling within the scope of the Medical Devices Directive.

The international standard EN/IEC 62304 has now emerged as a global benchmark for evaluating software development. This standard sits beside the following standards to evaluate the design, management and safety of medical software:

- EN/ISO 13485 (quality management systems).
- EN/ISO 14971 (application of risk management).
- IEC 60601-1 (medical electrical equipment safety).
- IEC 61010-1 (electrical equipment safety requirements).
- IEC 60601-2 (medical electrical equipment particular requirements).

The EN/IEC 62304 standard expects a manufacturer to assign a safety class to the software system. The classification is based on the potential for a hazard that could result in an injury to the user, the patient or other people and includes:

- Class A (no injury or damage to health is possible).
- Class B (non-serious injury is possible).
- Class C (death or serious injury is possible).
Similar to the EU device vigilance guidance, serious injury means injury or illness that, directly or indirectly:

- Is life threatening,
- Results in permanent impairment of a body function or permanent damage to a body structure,
- Necessitates medical or surgical intervention to prevent permanent impairment of a body function or permanent damage to a body structure.

In its 2012 guidance, the Commission clarifies the classification of stand-alone software and the conformity procedure to be followed. For example, stand-alone software that meets the definition of a medical device is considered as an active medical device. This means rules 9, 10, 11 and 12 of Annex IX to the Medical Devices Directive may apply. Clause 2.3 of the implementing rules in Annex IX provides that software which drives a medical device or influences the use of a device falls automatically into the same class as the device it drives. As regards software intended for diagnosis or therapy, according to rule 10 of Annex IX to the Medical Devices Directive, active devices intended for diagnosis are in Class IIa if they are intended to image in vivo distribution of radiopharmaceuticals.

For software that generates alarms based on the monitoring and analysis of patient specific physiological parameters (such as telemedicine systems), the communication system modules may be used with other modules that might qualify as medical devices. Similarly, where software is intended to capture and analyse results generated by one or more IVD devices, the software is considered as an IVD device. This includes, for example, software that integrates the genotype of multiple genes to predict a risk of developing a disease or medical condition.

**New regulatory framework**

In May 2008, a European consultation on medical devices was launched by the Commission.

Following the consultation, the Commission proposed a new regulatory framework for medical devices that will replace the three existing directives with two new regulations, one covering medical devices and the other covering IVD medical devices. The revisions come from a package of measures aimed at general medical devices and IVD medical devices to ensure safety and free movement of products and to deal with technical advances since the medical devices directives were drafted. The purpose of the proposals is to increase transparency, restore public confidence in medical devices, and harmonise the law in the EU.

The two draft regulations were proposed by the Commission on 26 September 2012. They are:

- Proposal for a Regulation of the European Parliament and of the Council on in vitro diagnostic medical devices (proposed In Vitro Diagnostic Medical Device Regulation).

The European Parliament adopted its first reading position of the draft proposals on 2 April 2014. Under the ordinary legislative procedure the European Parliament and the European Council must adopt the same final texts. Negotiations are under way, with trilogue meetings having taken place on 13 and 28 October, on 11 and 28 November and on 3 December 2015. Both proposed regulations are currently awaiting the Council's 1st reading position and budgetary conciliation convocation.

The following are the most significant changes in the proposals:

- The scope of regulated devices will be clarified and extended to include implants for aesthetic purposes.
- There will be stronger supervision of independent assessment bodies by national authorities.
- Notified Bodies will receive greater powers and obligations to ensure proper testing of medical devices and IVD medical devices and to conduct regular checks on manufacturers including without warning inspections of manufacturing sites.
- Only newly created special notified bodies will be able to issue CE certificates for high-risk devices such as implants.
- The rights and responsibilities for manufacturers, importers and distributors will be clarified and will apply to diagnostic services and Internet sales.
- The European Databank on Medical Devices (Eudamed) will be expanded to accommodate a new unique device identification (UDI) system required for labelling.
- There will be improved traceability of devices to allow for faster and more effective response to safety issues. Manufacturers will be required to have a “qualified person” responsible for regulatory compliance.
- The rules surrounding clinical investigations will be reinforced and clinical data will be required for medical devices and IVD medical devices both at the pre-market stage and as part of an ongoing assessment.
- Regulation of technological and scientific progress is to be adapted to new health technologies such as software and nanomaterial used in the provision of healthcare.
- Co-ordination between national surveillance authorities will be strengthened to improve the oversight of safety.
- The classification system for diagnostic IVD medical devices will be aligned with other medical devices by introducing a four-tier risk class system.
- A new expert group (the Medical Device Co-ordination Group) will be introduced that will have the power to review and comment on notified body assessments of high-risk medical devices before they are put on the market.

Stricter regulation and the conversion of three directives to two regulations should reduce inconsistencies between Notified Bodies. The UDI implementation and the Eudamed database expansion are designed to increase the safety of all devices.

**DATA PROTECTION**

**EU framework**

The growth of eHealth and mHealth raises a number of fundamental privacy concerns on the basis that both involve the processing (such as collection, recording and/or transfer) of information that includes personal data (such as information relating to a living individual who can be identified either from that information or in combination with information already held or available). Therefore, the use of eHealth and mHealth in Europe must be in compliance with:


The key provisions under the Data Protection Directive require that:

- Any processing of personal data is:
  - fair (the relevant individual about whom the data relates, be notified of the processing and reasons for it); and
  - lawful (the individual consents to the processing of their personal data, the processing is necessary for the purpose of a legitimate interest of the eHealth operator, or processing is necessary to protect the vital interests of the individual, such as in medical emergencies).

[global.practicallaw.com/lifesciences-guide](http://global.practicallaw.com/lifesciences-guide)
• Appropriate technical and organisational measures are taken against unauthorised or unlawful access to, or processing of, personal data and to protect personal data from accidental or unlawful loss, damage or destruction (this is particularly relevant for mHealth apps and devices which have the capacity to locally store large quantities of personal data but which may not have appropriate in-built safeguards).

• No personal data is transferred outside of the European Economic Area (EEA) unless the recipient country ensures “an adequate level of protection” (the use of cloud storage in relation to eHealth/mHealth information is of particular concern to European regulators as the storage of such cloud data is often outside the EEA, in the US or other jurisdictions).

The processing of information relating to a person’s health will likely include the processing of sensitive personal data (referred to in the Data Protection Directive as “special categories of data”), which has a greater level of legal protection. For example, the processing of sensitive personal data must likely be either:

• With the explicit consent of the relevant individual.

• Required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services.

Where the data is processed by a health professional or by another person, it would also be subject to an equivalent obligation of secrecy. eHealth operators will need to ensure these restrictions are adhered to in order to satisfy the legal requirements for processing such sensitive personal data.

In addition to the Data Protection Directive, the E-Privacy Directive contains specific rules regarding:

• Marketing communications.

• The storage or gaining of access to information stored in users’ equipment (such as by way of cookies and similar technologies).

• The security of communications services.

• Data breach notification.

• The privacy of traffic and location data.

The rules on storing/accessing information on a user’s device are not limited to personal data but any data on the device and such storage/access is only permitted if the user has given his consent.

EU member states have their own laws that adopt the provisions of the Data Protection Directive and E-Privacy Directive and in some jurisdictions these laws place more onerous restrictions or requirements on the processing of personal data. For examples of local variances, see below Differences and developments in key European markets.

Alongside the relevant legislative framework, regulators in the EU have issued guidance on the practical application of the law to real-world initiatives. These reinforce the fundamental concepts which data controllers must bear in mind when processing personal data in the context of mHealth and eHealth initiatives, such as “privacy by design and default” and the need to carry out privacy-impact assessments.

**Article 29 Working Party**

The Article 29 Working Party (AWP) is an advisory group made up of one representative from each of the data protection authority of each of the EU member states, the European Data Protection Supervisor and the Commission. Since 1997, the AWP has issued guidance in an effort to help organisations comply with the Data Protection Directive. Although the guidance is not binding, it can provide a helpful indication as to how data protection regulators will interpret and enforce the Data Protection Directive.

In 2007, the AWP produced a working document on the processing of personal data relating to health in electronic health records (see website, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf). It stated that health data should be interpreted as including any personal data closely linked to the health status of a person, such as genetic data or data on consumption of medicinal products or drugs, thereby expanding what would be treated as sensitive personal data.

**Apps on “smart devices”**

In February 2013, the AWP issued Opinion 02/2013 on apps on smart devices (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf). The opinion emphasises the requirement to provide clear and unambiguous information about processing to end users before app installation. In addition, the opinion reminds app developers of the need to:

• Obtain consent from the user (where the app in question stores or accesses data stored on the user’s device).

• Observe the principles of purpose limitation and data minimisation.

• Take adequate security measures.

• Observe reasonable retention periods.

• Observe fairness in the processing of data collected from and about children specifically.

**mHealth and eHealth and “Big Data”**

Another way in which the adoption of eHealth and mHealth technologies can raise privacy concerns is where information is used for “Big Data” analytics. “Big Data” is a term coined to mean a voluminous amount of unstructured data, a data set that is so large and complex that it cannot be processed using traditional database management techniques, but requires more sophisticated processing tools.

The idea of Big Data analytics is to mine this data, by using tools developed to manipulate and analyse the information in order to make quicker, novel and/or more intelligent decisions/findings. Organisations are naturally keen to use these techniques as they can provide valuable insight into the market, customers’ preferences and future trends. However, the potential benefits of Big Data to individuals (both individually and collectively) are also being recognised and it is being used more frequently, not necessarily for competitive gain, but for the public good, such as in the fight against deadly diseases.

The sources of Big Data may include:

• Internet search data and social media postings.

• Data collected by cameras, mobile phones and radio-frequency identification.

• Monitoring devices worn by patients in clinical trials or as devices connected to smartphones.

Much of the information collated may contain personal data and even sensitive personal data. In addition, new personal data can be created by Big Data analysis, such as by combining the test results of a clinical trial with information posted on social media about the patient’s lifestyle, in order to work out if they are likely to develop any medical conditions.

Where collating personal data for the purposes of Big Data, organisations must consider whether this would be expected by the relevant data subjects. Key questions to ask include:

• What were they told would be done with their data?

• Would they reasonably expect their personal data to be analysed/shared with another company for analysis in this way?

global.practicallaw.com/lifesciences-guide
Would the use of their data for Big Data analytics be incompatible with the reason(s) it was collected for in the first place (subject to exemptions)?

Transparency is key. In addition, the organisation must be confident that the information being used is adequate, relevant and not excessive for the proposed purposes. For example, does the name/address and so on of the data subject really need to be included to analyse the success of a new heart monitor being trialled? Can the data being collected be limited?

Organisations should also think carefully about the adequacy of the security steps they are taking. This is particularly relevant where the data being analysed is stored in a cloud, potentially hosted by a third party and potentially located outside the EEA (which raises concerns due to the laws in the host country), or where it is being shared with another organisation, to carry out the analysis.

In some cases, in particular where sensitive personal data is being used, the data subjects’ consent may need to be obtained. In others, the organisation may be able to demonstrate that the use for Big Data is necessary in the legitimate interests of that company (provided this causes no unwarranted prejudice for the individual). Local advice should always be obtained in relation to any specific queries on the lawful processing of sensitive personal data.

**General data protection regulation**

In acknowledgment of the fact that the Data Protection Directive is no longer fit for purpose for current technological standards, the Commission in 2012 published proposals to reform EU data protection laws.

The proposals focussed on a draft Regulation to replace the existing Data Protection Directive and seek to harmonise data protection compliance processes and enforcement across member states. The Regulation will have direct effect on organisations across all member states (that is, it does not need to be transposed locally to take effect, although departures from the Regulation are permitted in certain circumstances).

At the time of writing, the Council of the European Union has adopted a political agreement on the text of the Regulation which will undergo a legal-linguistic review and then be submitted for formal adoption by the Council and the European Parliament. Implementation is anticipated for summer 2018. The Regulation includes new definitions for ‘genetic data’, ‘biometric data’ and ‘data concerning health’. Such categories are included within the so-called “special categories of personal data” which are prohibited from being processed except in certain circumstances.

Processing of such data is permitted without the need for consent where the processing is necessary for public health purposes (which is broadly defined in the Regulation) and is in the public interest. EU member states are able to introduce further conditions with regard to the processing of genetic data, biometric data or health data as long as such conditions do not hamper the free flow of data within the EU. The Regulation introduces more prescriptive rules around how such data can be processed. However, the current draft also contains a helpful exemption for processing personal data for scientific research or public health purposes, in addition to a carve-out for tougher rules on profiling (including the need to carry out privacy impact assessments in most cases). While the proposals are likely to change over the coming months during the course of discussions between the EU institutions, the Regulation is anticipated to be agreed within the coming year.

**INTERPLAY WITH ELECTRONIC COMMERCE DIRECTIVE AND OTHER EU LEGAL INSTRUMENTS**

It has been recognised that eHealth or mHealth in the field of telemedicine is both a health service and an information society service. Therefore, it falls under Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Electronic Commerce Directive).

This is also recognised in Directive 2011/24/EU on the application of patients’ rights in cross-border healthcare (Cross-Border Healthcare Directive), which addresses patients’ cross-border mobility including their ability to access services across borders. The Cross-Border Healthcare Directive requires the Commission to take measures to ensure the inter-operability of the provision of eHealth services including tele-medicine.

The Court of Justice of the EU (CJEU) has ruled in various decisions that neither the special nature of health services nor the way in which they are organised or financed removes them from the regulatory control of the fundamental EU law principle of free movement. This includes the freedom of recipients of healthcare services established in one member state to seek and receive medical treatment from another member state, regardless of how the service is delivered (for example, by tele-medicine). EU law establishes a procedure that imposes an obligation on member states to notify the Commission and each other of all draft technical regulations concerning products and Information Society Services (ISS) including tele-medicine before they are adopted and put into operation in national law.

The E-Commerce Directive defines rules for the provision of ISS both within and between member states. According to the Commission, the E-Commerce Directive applies also to tele-medicine. For business-to-business tele-medicine services, the country of origin principle applies, meaning the service offered by the business must comply with the related rules of establishment. In the case of business-to-consumer activities, contractual obligations are exempted from the country of origin principle. In other words, the consumer may be protected by the laws of the country in which the consumer has their habitual residence.

While the definition of “medical activities” is a matter for the member states, as a general principle, the classification of specific tele-medicine services should ensure that these meet the same level of requirements as equivalent non tele-medicine services. That is to say, tele-radiology should not be less rigorous than radiology. This principle ensures that adequately regulated health services are not replaced by less regulated tele-medicine services, and it avoids discrimination between providers of the same service that would be incompatible with the E-Commerce Directive.

The interplay of the Medical Devices Directive and the Electronic Commerce Directive has recently been the subject of a CJEU decision (Case C-108/09 Ker-Optika bt v ÁNTSZ D4-durántüli Regionális Intézetet (Ker-Optika)). It has been argued that this decision supports the proposition that appliances or equipment intended for eHealth or mHealth would be subject to regulatory supervision under the Medical Devices Directive. However, this national decision gives some clarity on the demarcation between the Medical Devices Directive and the Electronic Commerce Directive, and the scope of the respective regulatory regime, particularly in the context of internet sale and supply of a medical device.

In addition, an assessment of the extent of impact of the Regulation relating to spectrum and radiofrequency use on devices intended for eHealth and mHealth is required. Currently, regulatory supervision generally falls within national competence.

In April 2014, the Commission launched its public consultation on the Green Paper which closed in January 2015. The Commission solicited views on how best to use mobile devices such as mobile phones, tablets, patient monitoring devices and other wireless devices to improve health and wellbeing. To realise the full potential of mHealth (which could save EUR99 billion in healthcare costs in the EU), the safety and usage of data and whether apps are medical devices must be addressed. Two open stakeholder meetings were held on 12 May and 6 July 2015. As regards classification, certain mHealth apps have now been classified as medical devices. In parallel, the Commission has published Section 77, which aims at the harmonisation of EU-wide standards, interoperability testing and certification of eHealth systems.
An important point raised during the consultation was the amount of mHealth apps on the market and the fact that they are unregulated, limiting their effectiveness and uptake by the public. The consultation and meetings concluded that to realise the full potential of mHealth apps it is important that they are able to be linked into electronic health records.

A working group on mHealth was formed in February 2016 and has been tasked with assessing the validity of data used in mHealth. The working group’s findings will be taken into account by the Commission in developing a policy to regulate the safety of mHealth apps. The working group includes research institutes such as Kings College London and the National University of Ireland, Dublin. The first meeting of the group is March 2016, and it is anticipated that guidelines will be finalised by the end of 2016.

**CONSUMER LAW CONSIDERATIONS**

Consumer law will also be relevant to mHealth projects. Directive 2011/83/EC on consumer rights (Consumer Directive) applies where an individual purchases an app relating to health/lifestyle/wellbeing. Such a purchase will form a “distance contract” between the trader and consumer and various rules governing cancellation and information requirements (see below) will be relevant.

The trader must provide the following information in a clear and comprehensible manner to the consumer before the conclusion of the contract:

- The main characteristics of the app.
- The identity of the trader and his contact details.
- The total price and any additional charges of the app.
- The arrangements for payment.
- Where a right of withdrawal exists, the conditions for exercising that right and the model cancellation form.
- Where a right of withdrawal does not exist, the information on that fact or the circumstances under which the consumer loses his right of withdrawal.
- The duration of the contract and in case of an indeterminate duration the conditions for terminating the contract.
- Where applicable, the minimum duration of the consumer’s obligations under the contract.
- The functionality of digital content, including applicable technical protection measures.
- Any relevant interoperability of digital content with hardware and software that the trader has to be aware of.
- Details of any relevant codes of conduct.

After the contract has been concluded, the trader must confirm the contract (which should incorporate the information above) on a durable medium.

**DIFFERENCES AND DEVELOPMENTS IN KEY EUROPEAN MARKETS**

**Belgium**

In Belgium, eHealth and mHealth are current issues which are being focused on and scrutinised by professional circles and other stakeholders, but also at the political and legislative level.

In addition to the transposition of the EU directives on medical devices and data protection, several legislative and pre-legislative initiatives have been taken in Belgium concerning eHealth and mHealth.

**Belgian legislation on medical devices.** The three EU directives on medical devices were transposed into Belgian law by the:

- Royal Decree of 18 March 1999 concerning medical devices.
- Royal Decree concerning active implantable medical devices.
- Royal Decree of 14 November 2011 concerning IVD medical devices.

These Royal Decrees set out rules relating to the safety and performance of medical devices under Belgian law. If an eHealth or mHealth feature falls within the scope of the conditions of a medical device, it falls into one of the classes provided by the applicable Royal Decree, depending on the characteristics and the risk assessment of the feature in question. If the feature falls under Class I, it must be notified to the Federal Agency for Medicines and Health Products (AFMPS/FAGG). Features of other classes must be assessed by the competent Notified Body. IVD medical devices are controlled by the Scientific Institute of Public Health (ISP/WIV).

In addition, a producer or any other person having such responsibilities must notify the competent authorities of any adverse incident relating to eHealth or mHealth, in accordance with the provisions of the EU Directives. Specific procedures for notifying complaints or incidents have been put in place and criminal sanctions have been provided for.

**Data protection (privacy).** The Data Protection Directive has been transposed into Belgian law by the:

- Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data (Privacy Act).
- Royal Decree of 13 February 2001 concerning the implementation of the law of the Privacy Act.

In addition, it may also be that the provisions of the Act of 22 August 2002 (Patients’ Act) relating to patient’s rights are applicable to eHealth or mHealth features. With the Patients’ Act, the Belgian legislator aimed to clarify the mutual rights and duties of patients and health professionals. The main principles laid down in the Patients’ Act are:

- The patient's freedom to choose a healthcare practitioner.
- The patient’s right to be informed of his personal health condition.
- The patient's informed consent for each intervention performed by the healthcare practitioner.
- The obligation for the healthcare professional to keep carefully updated health records.
- The protection of privacy.
- The possibility of lodging a complaint with the competent ombudsman in case of non-compliance.

**eHealth-platform.** The Act of 21 August 2008 on the establishment of an eHealth platform established a legal framework for dealing with several issues on eHealth in Belgium. The eHealth-platform is a public institution with legal personality with the mission to promote well organised e-services and information exchange and support between all actors in the healthcare sector. The eHealth-platform should provide necessary guarantees in terms of:

- Information security.
- Privacy protection of the patient and the healthcare professional.
- Medical secrecy.

Its aims are to:

- Optimise the quality and continuity of healthcare services.
- Optimise patients’ safety.
- Simplify administrative formalities for all players in the healthcare sector.

global.practicallaw.com/lifesciences-guide
• Provide a sound support for healthcare policy.
The eHealth-platform has been involved in the realisation of essential parts of the eHealth Action Plan 2013-2018 (see below), such as:
• Registration of software packages for healthcare professionals.
• Generalisation of e-prescription.
• Traceability of some implantable medical devices through a central register.

The eHealth Action Plan 2013-2018. On 22 October 2012, a Round Table Conference was held in Belgium between all concerned stakeholders (the competent authorities, several institutions and organisations and healthcare professionals). The objective was to come to a plan to create a more performant eHealth system, combining in a constructive and creative way the expertise and desires of all stakeholders. The Round Table Conference resulted in the adoption of an eHealth Action Plan to be rolled out over the period 2013-2018. 20 essential points were set out, including the creation of a global medical file, generalisation of e-prescription, traceability of some implantable medical devices through a central register and patient access to medical data.

In 2015, a second Round Table Conference was organised to evaluate progress and update the eHealth Action Plan 2013-2018. One of the newly included topics of the round table conference was mHealth. A working group (mHealth Working Group) was composed to prepare the discussions on mHealth and to draft a report for submission and discussion at two consolidation meetings in June 2015.

In its report, the mHealth Working Group first clarified what should be understood by "mHealth". According to the mHealth Working Group "mHealth" covers at least three types of applications:
• Tele-diagnosis (examination carried out remotely to diagnose the patient).
• Tele-monitoring (the processing of data generated by the patient).
• Tele-consultation (a virtual house call or consultation between healthcare professionals).

However, the mHealth Working Group did not examine issues such as responsibility, reimbursement, competent certifying authorities, informed consent and the business model for apps. Wellness and lifestyle apps were also not considered.

The mHealth Working Group first of all made clear that when it comes to the certification of apps and other telemedicine applications rules should be provided that deal with:
• Inter-operability.
• Privacy and security.
• The use of medical devices that are labelled and calibrated.
• Evidence based character.

The mHealth Working Group also pointed out that:
• National and international standards should be respected for data connections between the devices and platforms.
• Rules and standards for use of a protected access to platforms collecting data should be provided on the basis of the Privacy Act.
• Rules and standards for the encryption of medical data stored on mobile devices and platforms should be determined.
• Rules and standards for interoperability need to be set out.

On the use of smartphones and tablets specifically, the working group expressed its concern about safety risks (such as loss of the device, storage, encryption and authentication).

The results of all working groups of the Round Table Conference, including those of the mHealth Working Group, were bundled in a working document listing 20 action points. This document was officially confirmed by a Protocol agreed between the Ministers of the Inter-ministerial Conference for Public Health (Protocol) and published in the official Belgian Journal (Belgian Gazette) on 11 December 2015 (MB/BS, 12 December 2015, p. 7341B). The Protocol provides in actions, sub-actions and timing (from 2016-2018) for each of the 20 action points. For each action point or sub-action point an organisation and project leader is (to be) appointed. The organisations responsible for mHealth (action point no.19) are AFMPS/FAGG and the Belgian Institute for Social Security (INAMI/IREVI). By the end of 2016 a legal framework (including reimbursement conditions) should be in place. Five "use cases" have been withheld for support: stroke, cardiovascular care, diabetes, mental health and chronic pain.

Germany
Regulatory framework. There is no specific regulatory framework in place in Germany for the legal assessment of health information systems, mobile apps and software-based medical devices. The regulation of these products is therefore governed by the existing laws, in particular the Medical Devices Act (Medizinproduktgesetz). As regards health information systems, mobile apps and software-based medical devices, the question primarily arises as to whether the specific product falls under the scope of the Medical Devices Act. As under European law, this depends on whether the respective product is considered a medical device as defined under the Medical Devices Act.

Medical devices under the Medical Devices Act. In general, a product is classified as a medical device under the Medical Devices Act if it serves a medical purpose. Therefore, software can also be classified as a medical device if the software itself or the device for which it was programmed serves a relevant medical purpose. The required intended purpose is primarily defined by the manufacturer of the product. This means that a product is classified as a medical device if it is designed by the manufacturer to fulfil one of the following purposes:
• Diagnosis, prevention, monitoring, treatment or alleviation of a disease.
• Diagnosis, monitoring, treatment, alleviation or compensation for an injury or handicap.
• Investigation, replacement or modification of the anatomy or of a physiological process.
• Control of conception.

The Medical Devices Act therefore reflects the requirements of the Medical Devices Amendment Directive. The labelling of the product, the operating instructions and the underlying advertising material must be taken into account in assessing whether the manufacturer's product serves a medical purpose. This intended purpose cannot merely be avoided by a disclaimer from the manufacturer. Consequently, a manufacturer is bound by the information provided in the product labelling, operating instructions or advertising material.

This also means that the design of a product is not the only decisive factor in whether the product is considered a medical device under the Medical Devices Act. The manufacturer can clearly exclude the use of a product for a medical purpose and the mere fact that a product is suitable for one of the medical purposes does not make the product a medical device. The German Federal Supreme Court limits the right of the manufacturer to define the intended purpose of the product. The intended purpose as defined by the manufacturer is therefore only to be considered if it is not made arbitrarily. In this context, it is decisive whether a non-medical use
of the product is possible and could be considered reasonable. Such non-medical use may also exist if a product is designed for research purposes.

Software as a medical device under the Medical Devices Act. For the classification of software as a medical device, there are distinctions between different types of software, such as "embedded software", "accessory software" and "stand-alone software".

"Embedded software" forms an integral part of the medicinal product and is required for the proper use of the product. Therefore, the provisions of the Medical Devices Act also apply to the "embedded software" in a medicinal product as it is not possible to assess the software separately. A typical example of "embedded software" in relation to a medical device is the operating system of diagnosis or therapy devices.

This must be distinguished from software that is considered as an independent product in the form of an accessory to a medicinal product. In contrast to "embedded software" the medical device can principally also be used without the "accessory software", albeit with a limited range of functions. Such "accessory software" is also considered as an independent medical device if it is designed to be used together with a medical device. An example of "accessory software" would be image-processing software used in radiology, for example for highlighting certain shades in X-ray images.

Any software other than "embedded software" or "accessory software", such as "stand-alone software", can be regarded as a medical device if the software itself serves one of the stated medical purposes. For example, this is the case for software which analyses photographs of the user's skin, highlights skin changes requiring clarification and informs the user about such changes. Such software serves the purpose of diagnosis, prevention or monitoring of a disease (see above) and therefore constitutes a medical device. This would be different if the software merely captures images graphically and transmits them to a physician for further assessment as the purpose of the software would be limited to the capturing and transmission of image files.

Classification as a medicinal product. The consequences of a classification of a product as a medical device as defined under the German Medical Devices Act are complex and include that:

- Medical devices must be marked with a CE label. Such labelling only takes place if the medical device fulfils all European law requirements as well as the requirements of the German Medical Devices Regulation (Medizinprodukte-Verordnung), as determined in a formal conformity procedure.
- User information must be provided in the respective user's language.
- Medical devices cannot be placed on the market if there is a risk of danger to patients, users or third parties or if the manufacturer's performance information exceeds the actual performance capability of the medical device.
- The manufacturer must define the intended purpose and a risk classification must to take place.

Ireland Regulatory framework. Ireland is in a unique position in relation to this rapidly developing sector of the medical device industry. Ireland has promoted itself as a hub for both the medical device industry and the IT industry and, while it has been successful in doing so, its internal market for medical devices remains quite small. As such, the regulatory focus in Ireland over the past number of years has been to promote integration and interoperability, so as to open the Irish market up to the greater European market. eHealth has also been promoted as a way in which the Irish health system can drive efficiencies and control budgetary expansion.

The Active Implantable Medical Device Directive, the In Vitro Diagnostic Medical Device Directive and the Medical Device Directive have been implemented in Ireland through the following regulations:

- European Communities (Medical Devices Regulations) 1994 (SI 252/1994) (as amended).
- European Communities (In Vitro Diagnostic Medical Devices) Regulations 2001 (SI 304/2001) (as amended).

Ireland has not introduced specific legislation relating to health information systems, mobile apps or software based medical devices. Where Ireland has introduced regulations that go beyond what is required by the EU directives on medical devices, these have been introduced to either:

- Specifically deal with issues that have arisen concerning certain categories of medical devices, for example the problems relating to PIP breast implants,
- Increase the interoperability of the Irish medical device market with the European medical device market.

On 8 July 2014 the Health Identifiers Act 2014 was passed in to law in Ireland and became effective on 17 July 2015, following a ministerial order commencing the act. The Health Identifiers Act 2014 provides for each patient and healthcare provider to have a unique identifier, which will allow for greater portability of patient data both between healthcare providers and across multiple media. This is a key cornerstone of the Irish government's eHealth Strategy.

The Irish health service has also made a concerted effort towards using eHealth solutions in the Irish healthcare system. In 2015, the capital spending allocation in the health service for Information and Communication Technology was increased by 37.5%. eHealth Ireland is a new body which has also been established to promote the implementation of Ireland's eHealth Strategy and is currently working on implementing an Electronic Health Record System across the Irish healthcare system, so that patient data is readily transferable between healthcare providers in a secure manner, which it is hoped will lead to a nationally integrated healthcare system. These initiatives have formed part of a strategy pursued by the Irish government to promote the use and development of health information systems, mobile apps and software based medical devices, rather than to constrain the industry through further regulation.

Data protection. Ireland has not introduced any specific data protection legislation dealing with medical devices and, as such, the Data Protection Acts 1988 to 2003 (Data Protection Acts) apply to the processing and transfer of data via medical devices. The Data Protection Acts implement the provisions of the Data Protection Directive in Ireland. These acts will form the basis for the introduction of the European General Data Protection Regulation.

While there has been no specific data protection legislation introduced in Ireland to deal with medical devices, the Data Protection Commissioner of Ireland has issued non-binding guidelines on data protection in relation to research in the health sector, the Data Protection Guidelines on Research in the Health Sector (see website, www.dataprotection.ie/docs/Guidelines-on-research-in-the-Health-Sector(573).htm) (Guidelines). These provide medical device manufacturers with a useful guide to the best practices promoted by the Irish Data Protection Commissioner.

Under the Guidelines, where patient data is being processed for purposes not directly related to the patient's medical treatment, it is strongly recommended that either a pseudonym is used when
transferring data or that any factors which could link the data to the patient are removed before the data being transferred.

Where data concerning a patients’ medical treatment can be linked to a patient it is treated as sensitive personal data for the purposes of the Data Protection Acts and the patient’s explicit consent must be obtained before the data can be processed. Such consent must be freely given, specific, and the patient must be fully informed as to the purposes for which the data is to be used.

However, the Data Protection Acts provide for an exemption from the consent requirements for the processing of personal data for statistical, research or scientific purposes, if such processing is carried out by the data controller itself and the personal data is not disclosed to any third parties. This exemption is further limited in that it is only available where the processing of the personal data is not likely to cause damage or distress to the individual and can only be claimed by a data controller for research carried out by that data controller.

In addition to the consent requirements imposed by the Data Protection Acts, the Guidelines also require data controllers to put in place adequate safeguards to ensure that personal patient data is only used for the specified purposes for which it was provided.

**Italy**

**Italian legislation on medical devices.** The definition of “Medical Device” in Italian Legislative Decree 46/97 (as amended by Legislative Decree 37/2010), which implemented the EU directives on medical devices into national law, substantially resembles the one provided for by the EU directives. In particular, the medical devices definition also comprises software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and that is necessary for the proper application of a medical device.

The Ministerial Decree dated 22 September 2005 and issued by the Italian Health Minister introduced a National Classification of Medical Devices (NCMD), which groups medical devices under certain classification codes with the aim of facilitating the identification, processing, filing and communicating of data about medical devices. NCMD contemplated, among other things, several software types to be regarded as medical devices.

The Italian Ministry of Health and the regional health authorities are currently monitoring the forthcoming EU legislative developments on eHealth and mHealth, although Italian legislation has not yet confronted or regulated these topics.

On 20 February 2014, the Italian Ministry of Health issued national guidelines on eHealth outlining the need for the Italian public health system to:

- Properly train its operators on eHealth.
- Hire new professionals with capabilities in this field.
- Adopt cautionary measures when dealing with patients, who may not be familiar with technology.

**Data protection.** In Italy, the use of eHealth and mHealth complies with the Data Protection Directive, which was implemented in Italy by Legislative Decree 30 June 2003 n. 196 (Privacy Code). In addition, eHealth and mHealth must comply with further specific provisions and guidelines issued, from time to time, by the Italian Data Protection Authority (Authority) for specific sectors and/or data processing (for example the Guidelines on the Electronic Health Record and the Health File and the Guidelines on Online Examination Records).

The key obligations under the Privacy Code require that:

- Any processing of personal data is:
  - fair (that is the relevant individual about whom the data relates, be notified of the processing and reasons for it) and lawful (for example, the individual consents to the processing of their personal data (in writing if sensitive data is processed); or
  - necessary either to perform obligations resulting from a contract to which the data subject is a party, comply with specific requests made by the data subject before entering into a contract, protect the vital interests of the individual (such as medical emergencies), or where other conditions set forth by the law are met.
- Appropriate technical and organisational measures are taken against unauthorised or unlawful access to or processing of personal data and to protect personal data from accidental or unlawful loss, damage or destruction (this is particularly relevant for mHealth apps and devices which have the capacity to locally store large quantities of personal data but which do not have appropriate in-built safeguards).
- No personal data is transferred outside of the EEA unless the recipient jurisdictions have been deemed adequate by the Commission (the use of cloud storage in relation to eHealth/mHealth information is of particular concern to European regulators as the storage of such cloud data is often outside the EEA, in the US or other jurisdictions).
- The data controllers notify the Authority of the processing related to specific personal data, including:
  - genetic or biometric data or other data disclosing the geographic location of individuals or objects by means of an electronic communications network.
  - data disclosing health and sex life where processed for the purposes of assisted reproduction, provision of health care services via electronic networks and/or the supply of goods, epidemiological surveys, diagnosis of mental, infectious and epidemic diseases, seropositivity, organ and tissue transplantation and monitoring of health care expenditure.
  - data disclosing sex life and the psychological sphere where processed by not-for-profit associations, bodies or organisations of a political, philosophical, religious or trade-union character.
  - data processed with the help of electronic means with the purpose of profiling the data subject and/or his personality, analysing consumption patterns and/or choices, or monitoring use of electronic communications services except for such processing operations as are technically indispensable to deliver said services to users.

In this context, the Authority, aware of the new privacy issues arising from the proposed developments of the internet in which everyday objects would have network connectivity, including in relation to eHealth and mHealth, on 4 May 2015 launched a public consultation process to assess and define the measures and rules to ensure the maximum protection of users’ data. In particular, the consultation process is aimed at collecting information on how users are informed of their data processing and how their consent, if required, is collected and at assessing which measures (for example encryption or anonymity measures, certification tools and so on) should be adopted by the designers of software and/or “connected devices” producers to guarantee users’ privacy.

**Poland**

**Regulatory framework.** In Poland there is considerable interest in health information technology, eHealth and mHealth (together more commonly called “telemedicine”). Due to the rapid development of mobile technology, there are issues related to telemedicine that may raise doubts under the laws currently in force. Therefore, lately we observe numerous legislative and non-legislative initiatives and disputes in this matter.

**Medical devices.** The Medical Devices Act of 20 May 2010 implements EU Directives on Medical Devices, Active Implantable
Medical Devices and In-Vitro Medical Devices into the Polish law system. This law provides, among others:

- Rules for classification of the medical devices.
- Product-safety requirements.
- Steps of the safety assessment procedure.
- Supervision of the medical devices market.
- Notification of incidents.

In accordance with the definition of the medical device, standalone software can also be classified as a medical device. Therefore, if mobile applications, or other software intended use is of a medical nature (it diagnoses, monitors, cures, and so on) then such products fall under the scope of the Medical Devices Act.

The law differs for so called “self-control devices”, that is, in-vitro diagnostic medical devices that are intended to be used at home by a non-HCP and which provide results in relation to a given, examined patient. It is important for the producers and distributors of mobile devices that they verify whether their products fall under the scope of this definition.

Healthcare Information System and eHealth Platform. In Poland, the sharing of information between health services providers is regulated by the Healthcare Information System Act of 25 April 2011. Recently, its provisions did not allow exploiting the full potential of telemedicine (for example, standard paper medical documentation was still in use). Until mid-2017 amendments to the Healthcare Information System Act and other acts (among others, the Medical and Dentist Professions Act) will come into force. The amendments provide legal grounds necessary for implementation of the national healthcare ICT (the so called Project PI), which will allow:

- Patients to create their individual Internet Patient Account.
- Patients to access their treatment history and electronic medical documentation, including, among others, e-medical order, e-prescription, e-sick leave, and e-referral for a medical examination.
- Healthcare institutions to exchange patients' medical documentation (with their consent).

The above regulations and amendments to the Medical and Dentist Profession Act, allowing medical doctors to assess patient health using the ICT system or communication system, are a substantial step forward on a path to the common development of telemedicine.

The eHealth platform is still under construction. According to the new project timeline, it is anticipated that full functionality will be available in 2019 to 2020.

Spain

Spain was severely affected by the financial crisis, and as such has suffered a significant reduction in the resources (either private and public) available to it. As a result, the use of eHealth services in Spain is one the most significant in Europe. According to the 2014 Report on the Technology Information Society in Spain published by the Foundation of the Spanish Telecom Giant, Telefónica, it is envisaged that more than 42 million "wearables" offering functions related to health will be sold over the next year. In addition, there is considerable concern for privacy related to health information and so new data encryption systems are being implemented.

Spain has different regulations on health services as some competences are delegated to the Autonomous Communities. This gives a more complicated picture. National and regional authorities are very keen to develop more effective and less costly services for patients. One of the key projects the Spanish Ministry of Health is currently developing consists of a centralised database system for use by all the Autonomous Communities to provide the same services in all the territories with the same levels of data for all patients. This system is creating a uniformed data system (called the Database of the National Public Health System) where the information concerning a patient's file, electronic records, online appointment and e-learning, among others, will be shared with healthcare professionals (HCPs) and patients' data files in the same manner regardless of where they are.

The Advisory Health Board issued a Report in April 2014 focusing on the development of eHealth services as a key priority for the Spanish Health System. This Report proposed a harmonised legal framework for eHealth and mHealth as a growth vehicle alongside the Investigation and technological improvement of areas such as the biotechnological and electronic sectors and the collaboration between public authorities and private investors.

Recent developments also include:

- Madrid's Telemedicine Plan 2014-2018 (Plan de Telemedicina) which will facilitate health assistance and reduce barriers to access those health services.
- The report published in March 2015 "Index SEIS 2014" of the Spanish Society of Health Informatics (Sociedad Española de Informática de la Salud), which aims to analyse the strategic lines on Information and Communications Technology for Health in Spain.
- The incorporation in March 2015 of the Iberian Society of Telemedicine and Teleconsultation (Sociedad Iberica de Telemedicina y Teleconsultación), which aims to promote and spread the benefits of the eHealth.

In relation to mHealth (or mobile apps), there is an increasing number of outsourcing companies that are developing management systems for chronic patients and personalised health services or apps aimed at earlier detection of illnesses for big pharmaceutical companies.

These technological advances and improvements in eHealth services have not been accompanied by a sectoral and specific regulation of the key issues affecting this area, such as data protection, intellectual property protection, patient security, product liability and professional negligence. Those areas are regulated by general laws (the Data Protection Act, Intellectual Property Law and Consumer Act, among others) which do not specifically cover this particular and advanced sector. Future legal developments in this area should cover the security of personal data to avoid any undesired transfer or manipulation, and the security of the apps as a key issue to help foster patient trust in this new technology.

UK

The research exemption. The Data Protection Act 1998 (DPA) gives an exemption which is potentially useful for organisations processing personal data for mHealth and eHealth purposes. This exemption allows the processing of personal data where the data is processed for something other than what it was collected for (and therefore, the purpose is incompatible with such original purpose and in breach of the Data Protection Directive), but the organisation now intends to use it for research purposes. "Research" is not defined, but it is likely to include research for scientific purposes. If the research is used to make a decision affecting an individual or is likely to cause substantial damage or distress to an individual, then the exemption would not apply. For example, it would not apply where research data obtained through a drug trial (containing sensitive personal non-anonymised data) was shared with insurance companies without the volunteers' knowledge to allow those companies to use the data to alter the volunteers' insurance premiums or send tailored marketing for particular medical insurance products to those individuals. If the exemption applies, it does not provide a free hand with regard to the use of the data and many of the requirements under the DPA will still be relevant. Caution is therefore required when intending to rely on this exemption.
Care.data. In the UK, the use of personal data (including Big Data analysis) for medical purposes has been the topic of discussion and heated debate in the context of the UK government's proposed implementation of the NHS care.data scheme, designed to allow analysis of health information collected by GPs on an unprecedented scale. The aim of the initiative is to provide joined-up information about the care received from all of the different parts of the health service, including hospitals and GP practices. The intention is for any such studies to be carried out on an anonymous basis, but there have been widespread concerns raised regarding the true anonymity of the data extracted from these records and whether patients' wishes to opt-out of the scheme altogether have been respected.

Information Commissioner's Office (ICO) guidance on mobile apps. In December 2013, the ICO launched new guidance for app developers to help combat the public's perception that personal information collected through apps is not being appropriately protected under the DPA.

The guidance includes commentary on the following:

- Identifying personal data, that is, not just name or image but also information such as IMEI numbers, MAC address and mobile phone numbers.
- Determining who is the data controller.
- Data minimisation, that is, collecting a minimum amount of data to the extent necessary for the performance of the app.
- Privacy impact assessments (PIA). Developers should consider publishing the completed assessment, but should also regularly review and re-publish.
- “Privacy by design”, ensuring that data protection is a high priority when developing the app and as such ingrained in its framework.

- “Layered privacy notices”. So as not to weaken the user experience, the idea is to provided information in layers, if the user wants further information they can click on a link for more details.
- Transparency information about the processing of users' personal information should be presented before any personal information is collected, and important information should not be hidden and developers should not try to mislead users.
- The use of “just-in-time” prompts to notify users when certain actions have particularly intrusive privacy implications, such as when geo-location information is being collected.
- The use of advertising, which must be clear to users, as well as the use of any analytics in the app.
- Encryption. Where storing data for later use or transmitting usernames, passwords and any particularly sensitive information, only established cryptographic methods and codes should be used.

In particular, the ICO will look carefully at who is controlling the purposes for which data is collected and the means of collection. Developers, apps stores and platform providers therefore need to consider very carefully what capacity they are dealing with any personal data (if at all).

Consumer Rights Act 2015. The Consumer Rights Act 2015 (CRA) received Royal Assent on 26 March 2015 and came mostly into force on 1 October 2015. The CRA sets out a framework that consolidates in one place key UK consumer rights covering contracts for the supply of goods, services and digital content, and the law relating to unfair terms in consumer contracts.

The CRA is the first piece of legislation to regulate the supply of digital content (which would include health/wellbeing apps) and introduces tailored quality rights for digital content and tailored remedies if the digital content rights are not met.

In summary, the CRA:

- Introduces certain statutory implied terms and remedies in consumer contracts for goods, digital content and services.
- Requires that pre-contract information required under the consumer contracts regulations must include terms that are automatically implied into a contract with a consumer.
- Clarifies when terms and conditions can be considered unfair.

Organisations selling m-health apps to consumers should be reviewing and updating their internal and consumer-facing processes and documentation, including sales processes, cancellation policies and consumer supply terms (including app supply terms), to ensure compliance with the CRA.

FUTURE REGULATION

The rate of development of integrated health information systems, mobile apps and software based medical devices has created a degree of uncertainty as to whether some of these new technologies fall within the existing regulatory framework for medical devices. This next generation of medical devices are bridging the gap between the traditional medical device sector and the e-commerce and telecommunications sectors. As such, regulatory responsibility for such devices will no longer fall exclusively with the medical device regulatory regime but will also become increasingly subject to data protection regulation and e-commerce regulation.

As outlined above, when introduced, the proposed Medical Device Regulation and proposed In Vitro Diagnostic Medical Device Regulation will update the current regulatory environment for medical devices and will address a number of shortcomings identified in the current regulatory regime. Rather than radically overhauling the current regime, the proposed regulations aim to build on the foundations already in place.

The proposed regulations do not attempt to redefine what is a medical device or an in vitro medical device. However, when introduced they will provide for greater flexibility in determining whether a device fits within the existing definitions by allowing member states to request a decision from the Commission as to whether the regulations apply. To aid the Commission in determining this, the proposed regulations will establish a new expert committee, to be known as the Medical Device Co-ordination Group (MDCG), which will be made up of members from each member state. The MDCG will advise the Commission, who, on receipt of a request from a member state, will decide on a case-by-case basis whether a specific product or piece of software, or specific group of products or software, falls under the proposed regulation.

Such a procedure will provide the proposed regulations and flexibility required to adapt to the rapid technological development in this area. To date, the Commission has relied on non-legally binding guidance to provide greater clarity, whereas the proposed regulations will allow the Commission to provide legally binding decisions that will apply across all member states. This will promote greater harmonisation across member states and provide greater legal certainty for manufacturers and developers.

Another key innovation to be introduced under the Proposed Regulations is the introduction of a unique device identification (UDI) system. Any device which is deemed to be a medical device or an in vitro medical device for the purpose of the regulation will be required to a unique identification code. This will allow for greater tractability of devices and help to foster consumer confidence, as the UDI will allow for better reporting and corrective actions where faulty devices are released onto the market.

Another key element which will have a profound impact on the pace at which health information systems, mobile apps and software based medical devices develop in the European market will be the integration of health care markets across Europe, which have traditionally remained member state specific. The Cross-
Border Healthcare Directive was an important first step in this process. This directive sets out the positive intention of the EU to support the development of eHealth across the EU, and to facilitate the exchange of information among member states. The directive provides for, among other things, the recognition of prescriptions across member states and the creation of European reference networks, whereby healthcare professionals from various member states can share information in relation to rare diseases. This interoperability between health care systems and increased portability of medical data will help to foster development in the medical device market and provide growth opportunities for the next generation of medical devices.

The drive at an EU level towards a digital single market will also have an important impact on the future growth of mobile apps and software based medical devices across Europe. In its communication, A Digital Single Market Strategy for Europe (see website, http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf), the Commission stressed the importance of breaking down the cross border barriers that remain in the digital marketplace. While currently there have been no new legislative proposals put forward to liberalise further the European digital marketplace it is an area that the Commission has identified as requiring further reform and an area in which future regulations are likely to affect the next generation of mobile medical devices. This coupled with the concerted drive over the past number of years to provide for cheap and effective data roaming across member states will aid the development of this sector of medical devices.

RECENT DEVELOPMENTS
As a result of the stakeholder meetings on 12 May and 6 July 2015 a series of developments were announced:

- The Commission has proposed a code of conduct (see website, http://ec.europa.eu/digital-agenda/en/news/mhealth-green-paper-next-steps) for mHealth mobile apps that will cover data privacy and security best practices.
- The British Standards Institute has published a code of practice on health and wellness apps (see website, http://shop.bsigroup.com/forms/PASs/PAS-2772015] which covers adequacy for purpose, quality, safety and the life-cycle management of mHealth apps.
- The European Data Protection Supervisor has published an opinion on mobile health (see website, https://secure.edps.europa.eu/EDPSWEB/edps/EDPS) that argues that all mHealth apps should offer users a custom setting that prevents remote processing, storage and backup of their data.
- The French Data Protection Authority, CNIL, has announced mHealth as a priority enforcement area (see website, www.cnil.fr/institution/actualite/article/article/programmes-controles-2015).

We expect the mHealth working group to produce a policy to regulate the safety of mHealth apps and some guidelines before the end of 2016.

Often, health IT companies find that they are ill-prepared to meet developing regulatory challenges. It is recommended that companies venturing into the health IT area invest at the early stages in developing a strong understanding of the legal and regulatory issues, and associated investments and timelines, for proposed products before developing the technology or making improvements to existing technology. Such companies must plan to invest in the infrastructure and processes necessary to ensure that regulated health IT remains compliant. A coherent and integrated commercial strategy for the development of devices relevant to eHealth and mHealth should be considered on a cross-border basis.

This article includes contributions from Gunther Meyer (Belgium), John Coary (Ireland), Marta Gadomska-Golab (Poland), Beatrice Bigonzi (Italy), Lizzié Charlton (UK), Tobias Maier (Germany) and Eduardo Buitron (Spain).

Practical Law Contributor profile

Simon Crossley, Partner/Sector Group Leader: Health & Life Sciences
Eversheds LLP
T +44 20 344 33502
F +44 20 344 33777
E simon.crossley@eversheds.com
W eversheds.com


Non-professional qualifications. Degree in Chemistry/Biochemistry.

Areas of practice. Intellectual property, licensing, life sciences regulatory and technology transfer.

global.practicallaw.com/lifesciences-guide