The Impact of Artificial Intelligence on Medical Innovation in the European Union and United States

By Lincoln Tsang, Daniel A. Kracov, Jacqueline Mulryne, Louise Strom, Nancy Perkins, Richard Dickinson, Victoria M. Wallace, and Bethan Jones

Artificial intelligence (AI) software means computer programs with the capacity to perform operations analogous to learning and decisions-making in humans. This tool is being increasingly applied in the pharmaceutical, medical device, and healthcare sectors to aid various stages of research and development, as well as treatment of patients. AI software, and in particular software that incorporates machine learning, which provides the ability to learn from data without rule-based programming, may streamline the process of translating a molecule from initial inception to a market-ready product.

Drug discovery is a lengthy and costly process, and any technology capable of improving the efficiency of drug development is always desirable. Further, enabling companies to process and analyze large amounts of data generated post-market can mean better insight into how an innovative product works in the real world, and so improve knowledge and accuracy of treatment choices. Given the sector is highly regulated, these technological advances may bring about significant legal and regulatory policy challenges in view of the convergence of biological, physical, and mathematical sciences. We set out below how AI may contribute to the research and development of health products, to the care and treatment of patients, and the corresponding legal and regulatory issues surrounding such technological advances.

Application of Artificial Intelligence Software to Medical Innovation

To meet the societal and patient needs of the 21st Century, current drug development will need to dramatically improve in efficiency. AI, as a form of machine learning in particular, presents the pharmaceutical industry with a real opportunity to revolutionize research and development programs, especially at the earliest stages of product development in screening for potential drug targets and the corresponding drug candidates.

For example, BenevolentBio, a company focusing on research in amyotrophic lateral sclerosis, relies on a Judgement Correlation System (JACS) to review and assess relationships between millions of scientific research papers and abstracts in order to generate novel hypotheses, which are then assessed by researchers.[1] Similarly, the University of Manchester in the United Kingdom has developed an AI platform titled "Eve," which is capable of screening more than 10,000 compounds per day, and matches them to likely targets. The program improves in tandem with Eve's progressive learning of successful screening, and thereby helps improve the precision and accuracy of drug candidate identification.[2]

A further example is BERG's AI "Interrogative Biology," which is capable of examining 14 trillion data points in a single tissue sample. BERG extracted biological data from healthy and cancerous tissue samples from over 1,000 patients. The data were then processed and analyzed by AI algorithms, which suggested possible drug treatments. According to the company, it would be impossible to manually process the volume of source data, and to understand what they meant in biological and disease terms, without the help of AI.[3]

While these uses save companies time and money, the AI applications that have received the most interest in the trade press are related to its application for improving care and treatment of patients, as well as encouraging greater patient engagement. A computer system, "Physiscore," analyzes real-time data routinely collected in neonatal intensive

Lincoln Tsang, Daniel A. Kracov, Jacqueline Mulryne, Louise Strom, Nancy Perkins, Richard Dickinson,Victoria M. Wallace, and Bethan Jones are members of the Global Life Sciences Practice of Arnold & Porter Kaye Scholer LLP.

Published in the August 2017 issue of the *Intellectual Property & Technology Law Journal*

care units (such as heart rate, respiratory rate, and oxygen saturation) alongside other inputs (such as birth weight and gestational age) to predict whether premature babies are likely to have health issues. Physiscore was found to outperform all other available detection methods, including manual assessment.[4] Houston Methodist Research Institute has developed a program that will facilitate earlier diagnosis of individual's susceptibility to developing breast cancer. The software program analyzes mammograms and translates patient data into diagnostic information 30 times faster than a healthcare practitioner, and with 99 percent accuracy.[5] IBM's supercomputer, nicknamed "Watson," has been used to scan genetic data from the tumors of brain cancer patients, reducing the time taken to do so from weeks or months to only minutes. Data on individual patients' mutations can then be matched to tailored clinical treatment plans.[6]

There also are exciting developments in the areas of patient care and disease management. For example, Medtronic and Johnson & Johnson entered into Watson Health partnerships with IBM in April 2015 with the respective aims of using AI to personalize diabetes management solutions[7] and to set up mobile-based coaching systems for pre- and post-operative patient care.[8] Novo Nordisk has also signed up to an IBM Watson partnership, to launch a digital platform to help manage patients' diabetes by monitoring and analyzing data concerning patients' blood sugar levels, food intake, and medicine usage[9] in real time, thus enabling diabetes patients and their doctors to respond more quickly to peaks and troughs in blood sugar.

AI has been exploited post-market in the life science sector. There is a greater demand by regulatory authorities for manufacturers to generate and analyze a significant amount of data relating to safety, quality, and clinical effectiveness after product approval. AI has the potential to streamline this process. For example, manufacturers are expected to improve continuously the methods used for the manufacture and control of marketed products to minimize variability in the product that may be attributed to variations in clinical performance. Shire has embraced these machine-learned manufacturing potentials by making use of Statistica to control access to validated, real-time process data and analytics in support of its manufacturing operations.[10]

Machine learning tools also could be used to predict the occurrence of adverse events in particular patient subpopulations. For example, a partnership was struck between Celgene and IBM in November 2016 seeking to monitor the safe and effective conditions of use of products through the creation of a cloud-based drug evaluation platform, to be run on IBM Watson.[11] In June 2016, GlaxoSmithKline's (GSK) consumer business for over-the-counter (OTC) products announced a collaboration with IBM Watson. The aim of the collaboration is to interact with consumers through GSK's online ads,[12] thus helping consumers make "more informed decisions at the point of consideration." On October 6, 2016, GSK announced that the use of Watson's interactive functionality had been launched for the company's Theraflu brand, which covers a range of OTC products to relieve the symptoms of pain, sinus congestion, runny nose, sneezing, and cough due to colds, upper respiratory infections, and allergies.[13]

While these opportunities are being explored by companies and healthcare professionals alike, before AI is adopted for general application in clinical practice, or for use in drug research and development, the technology will need to be verified and validated in terms of its reliability, accuracy, and cost-utility.

Policy Initiatives

In addition to the private sector's increasing use and development of AI software, policy makers and governments are considering the technology's value and applicability.

In the European Union (EU) for example, the European Commission has identified robotics and AI as cornerstone technologies, and has recognized the need for significant investment in this area. The need for novel approaches and skills to tackle the associated hurdles, including legal challenges, has been acknowledged. To this end, a new EU taskforce recently was established by the European Commission, which will examine obstacles to the adoption of big data and digital technologies in healthcare. The initiative is borne out of frustration that Europe's healthcare systems continue to fail to garner the benefits of new digital technologies. The taskforce is due to present policy proposals to accelerate the use of genomics data in research and maximize the potential of big data analytics to interrogate health data. These endeavors are likely to reduce lead-times for the introduction of new treatments and enable more personalized healthcare.

Compliance Issues Arising from Application of AI to Medical Technologies

Medical devices and technology used within the medical sphere often are highly regulated. Regulatory authorities aim to ensure that products are safe and efficacious, and that any data generated products, and any data generated in connection with development or use of the products, are accurate and can be relied on to inform treatment choices and ensure the

products are used safely and effectively. Consumers are also concerned that their personal data are collected, analyzed, and used properly. With this in mind, we set out below an overview of the current regulatory framework in the EU and the United States.

Europe

Current Regulation of Software in the European Union

Not all software used in the healthcare setting is considered to be a medical device. However, depending on its functionality, and its intended purpose, software may fall within the EU definition of "medical device." Product classification is determined according to the requirements set out in Directive 93/42/EEC (the Directive).[14] Article 1(2) of the Directive provides that a medical device means any instrument or other apparatus, including software, intended by the manufacturer to be used for human beings for the purpose of, among other things, diagnosis, prevention, monitoring, treatment, or alleviation of disease. Software may be regulated as a medical device if it has a medical purpose as assigned by the manufacturer. European courts have ruled that a medical purpose covers an object intended by its manufacturer to be capable of appreciably restoring, correcting, or modifying physiological functions in human beings.[15]

The assessment takes account of the product's composition, the manner in which it is used, the extent of its distribution, its familiarity to consumers, and the risks which its use may entail.[16] Classification of software is fraught with practical challenges because, unlike classification of general medical devices, it is not immediately apparent how these parameters apply to software, given that software does not ordinarily act on the human body to restore, correct or modify bodily functions.

The European Commission has published guidelines to interpret requirement set out in the Directive (the MEDDEVs).[17] Although MEDDEVs are not legally binding, they nonetheless represent the agreed position of the European Commission, the national competent authorities, and industry on how the legal requirements are interpreted and workably put into practice. Moreover, in the first case to be heard by the Court of Justice of the European Union (CJEU) regarding classification of software in the context of medical devices legislation, the Advocate General recently endorsed the MEDDEVS.[18] The CJEU will now consider this opinion and deliver a judgment in due course. While the Advocate General's opinion is not binding on the CJEU, it does help to clarify how to apply the existing regulatory criteria to medical software pending the CJEU's decision.

For example, software that calculates anatomical sites of the body, and image enhancing software intended for diagnostic purposes, generally is viewed as a software medical device because it is used as a tool, over and above the healthcare professionals' clinical judgment, in order to assist clinical diagnosis and treatment. In contrast, software used for administration of general patient data, or information systems intended only to store, archive and transfer data, and programs that alter patient data for embellishment purposes, do not render the software a medical device.

In relation to AI specifically, programs that analyze large amounts of data to develop knowledge about a disease or condition, rather than to decide on treatment options for an individual patient, may not necessarily be considered as having a medical purpose, and hence as a medical device. In contrast, AI aimed at enhancing or improving clinical diagnosis or informing decisions on treatment likely will be considered as having a medical purpose if the software is designed as a tool beyond data capture and communication.

In addition, the European Commission is developing guidelines on mobile health apps and software irrespective of whether they are classified as medical devices. Draft guidelines have been published to assess the validity and reliability of data collected and processed by health and wellbeing apps, and are currently being discussed by stakeholders.[19] These draft guidelines aim to establish a common set of criteria relating to quality, safety, reliability, and effectiveness to underpin the methodologies that can be used for assessing health apps. The sector non-specific guidelines, when adopted, will be voluntary. That said, they are nonetheless important to guide good practice in developing software in the healthcare sector, and are likely to serve as a useful reference for AI developers.

EU Regulation of Software under the New Medical Device Regulations

Following a lengthy legislative process, a new medical device regulation (the Regulations) has replaced the Directive,[20] and the new rules will apply as of May 26, 2020. The Regulations contain additional provisions that specifically address software medical devices. Of particular relevance, software with a medical purpose of "prediction and prognosis" will fall within the scope of the Regulations. This means that AI software that currently are excluded from being regulated as software medical devices under the existing regulatory regime, because they do not provide a treatment recommendation, but only a prediction of risk to or predisposition of a disease, may in the future be re-classified as medical devices.

Data Protection and Cybersecurity Implications

Data protection in the EU currently is governed by Directive 95/46/EC, which requires implementation in each Member State. To modernize the data protection framework in the EU, a General Data Protection Regulation[21] (GDPR) has been adopted and will apply directly in all Member States from May 25, 2018.

The use of AI software raises data protection implications and has prompted some data protection regulators to issue updated guidance on how the technology can be used in a way that is compliant with data protection legislation. Certain aspects of the legislation are particularly relevant to AI software. One of these is the principle of "accountability," which is an implicit requirement under the current law but has been explicitly introduced in the GDPR. The GDPR's accountability principle[22] requires organizations to demonstrate compliance with all the other principles in the GDPR, and several further provisions of the GDPR also promote accountability. In particular, records of the purpose of processing activities must be maintained in certain circumstances when organizations process personal data that could result in a risk to individuals' rights and freedoms.[23] This may prove to be a difficult requirement for organizations that utilize AI software to meet, as the ultimate purpose of data analysis is not always known at the outset and may change in tandem with discovery of new correlations in the data. Similarly, organizations are required to implement security measures that are "appropriate to the risk" involved in the processing of that data.[24] For organizations that utilize AI software, where the level of risk often evolves in parallel with the AI's use, this may be a difficult requirement to adequately comply with.

Organizations often rely on individuals' consent to legitimize the processing of personal data and the requirements for consent are tightened in the GDPR.[25] The nature of AI techniques means that it can be difficult for meaningful consent to be obtained from relevant individuals. Organizations that use AI software may therefore need to think about more innovative ways of obtaining consent where necessary, such as by obtaining consent from individuals at various stages throughout the use of the software, or exploring how software agents could provide consent on behalf of individuals.

Organizations looking to use AI software could also try to establish legitimate interests for carrying out any related personal data processing, so would need to evaluate how the software analytics could potentially affect people's privacy and balance that against the organization's objectives.

A further challenge associated with the GDPR is the right to be given an explanation by a natural person of decisions based on automated processing.[26] The outcome of machine learning algorithms may not be easily rationalized by the humans that rely on them, especially when decisions are made as a result of enormous compilations of data. In these circumstances, it may not be possible to give a more meaningful explanation than a description of the processes used and the categories of data that have been fed into it.

To try to manage the new questions that the use of AI software raises from a data protection perspective, Ministers of the European Parliament (MEPs) asked the European Commission to propose EU-wide rules on robotics and AI in February 2017. They proposed a voluntary code of conduct for researchers and designers to sign up to, to confirm that they operate in accordance with regulatory standards and respect human dignity. In addition, the MEPs asked the European Commission to consider establishing a European agency for AI, to provide guidance to public authorities. The resolution was passed by 396 votes to 123. Although not binding on the European Commission, the Commission would need to justify any departure from the recommendations.

To prevent unauthorized use of personal data collated through AI software, it also is crucial to have in place measures to combat cybersecurity vulnerabilities. To this end, the EU recently has adopted a Cybersecurity Directive[27] that must be implemented in the national legislation of EU member states by May 10, 2018. The Cybersecurity Directive imposes obligations on EU member states to adopt a network and information security strategy, and to designate a competent authority to implement and enforce the Directive. There are also obligations placed on essential services operators (including, in particular, public or private entities in the healthcare sector) and digital service providers (including cloud computing services) to take various security steps, such as implementing risk management practices and reporting major incidents to the relevant national authority.

United States

Regulation of Software in the United States

As advances in AI pave the way for developments in medical technologies, exactly how the AI will be regulated in the United States largely will be a function of its intended use. One key question for AI developers is whether the AI will be considered a medical device and thus fall within the Food and Drug Administration's (FDA's) regulatory jurisdiction.

In the United States, the Federal Food, Drug, and Cosmetic Act gives FDA regulatory authority over medical devices. FDA considers a medical device to be an instrument

or other apparatus, component, or accessory that is *intended* for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease in man or other animals, or that is *intended* to affect the structure or function of any man or other animal but which is not dependent on being metabolized *(i.e.*, a drug) for achievement of that purpose. [28] Thus, FDA takes an intent-based approach to determine whether a product is regulated as a medical device. Intended use refers to objective intent, and to determine this intent FDA may take into account "any claim or statement made by or behalf of a manufacturer that explicitly or implicitly promotes a product for a particular use."[29] Products that meet FDA's definition, and are not otherwise exempted from FDA jurisdiction by statute, are then placed on a "regulatory continuum" and classified into Class I, II, or III. Device classification depends on the intended use of the device, its indications for use, and the risk the device poses (with Class III including those with the greatest risk). Regulatory control increases from Class I to Class III, ranging from an FDA exercise of enforcement discretion, to an exemption from clearance, to a 510(k) premarket notification, to a full premarket approval application requirement.

Of most relevance for AI developers are the four general "categories" of FDA regulated software:

1. Mobile Medical Apps (MMAs);
2. Medical Device Data Systems (MDDS);
3. Software as a Medical Device (SAMD); and
4. Clinical Decision Support Software (CDSS).

Depending on its "category," a product may not be a medical device at all, may be subject to enforcement discretion, or may be a Class I, II, or III device.

For Mobile Medical Apps, there are three categories of apps: (1) Apps that are not medical devices; (2) apps subject to "enforcement discretion;" and (3) apps that are fully regulated medical devices. According to its 2015 Guidance on MMAs, FDA intends to apply its regulatory authority to select software applications "that are medical devices and whose functionality could pose a risk to a patient's safety if the mobile app were to not function as intended."[30] This includes mobile apps that conduct patient-specific analysis and provide patient-specific diagnosis, or treatment recommendations *(e.g.*, an app that uses patient-specific parameters and calculates dosage or create a dosage plan for radiation therapy).

Medical Device Data Systems are those systems intended to provide electronic transfer, storage, format conversion, or display of medical device data without controlling or altering the functions or parameters of any connected medical devices.[31] On February 15, 2011, FDA down-classified MDDS from Class III (high-risk) to Class I (low-risk) and on February 9, 2015, FDA issued Guidance stating that it would exercise "enforcement discretion" for MDDS.[32]

Regarding SAMD and CDSS, regulatory status and classification decisions focus on the type of information being analyzed and how information is converted. FDA has defined SAMD as "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device."[33] CDSS is software that utilizes patient information to assist providers in making diagnostic or treatment decisions, such as IBM's Watson.

Until recently, in the United States, software was approached by FDA using the regulatory continuum described above. However, enacted in 2016, the 21st Century Cures Act legislatively exempts certain software from the definition of a medical device. Specifically, the Act clarifies that the term "device" does not include a software function that is intended:

- for administrative support of a healthcare facility *(e.g.*, billing);
- for general health maintenance;
- to serve as an electronic patient record system *(e.g.*, Electronic Health Records); or
- for transferring, storing, converting clinical laboratory, or other device data results (already subject to FDA enforcement discretion).[34]

Additionally, as relevant for CDSS, the law excludes from the definition of "device," software (unless the software is intended to "acquire, process, or analyze a medical image or a signal from an in vitro diagnostic device or a pattern or signal from a signal acquisition system"):

- Displaying, analyzing, or printing medical information about a patient or other medical information (such as peer-reviewed clinical studies and clinical practice guidelines);
- Supporting or providing recommendations to a healthcare professional about prevention, diagnosis, or treatment of a disease or condition; and

- Enabling healthcare professionals to independently review the basis for such recommendations so that the software is not primarily relied on to make a clinical diagnosis or treatment decision regarding an individual patient.[35]

Thus the Act generally excludes most CDSS from FDA jurisdiction. However, it is worth noting that the FDA may bring CDSS back under its jurisdiction if it makes certain findings regarding:

- the likelihood and severity of patient harm if the software does not perform as intended;
- the extent to which the software is intended to support the clinical judgment of a healthcare professional;
- whether there is a reasonable opportunity for a healthcare professional to review the basis of the information or treatment recommendation; and
- the intended user and use environment.[36]

Additionally, as AI advances and becomes capable of making or altering medical diagnoses or treatment decisions, with little input or oversight from physicians or transparency as to underlying assumptions and algorithms, these technologies will fall outside of the 21st Century Cures Act's exclusion. It will be interesting to see the way the FDA approaches AI, and if other agencies step up their scrutiny of such systems. Recently, the FDA announced that it is assembling a new Digital Health Unit, comprised of computer scientists and engineers, to prepare for future developments in AI-driven medical software.[37] The unit will provide technical assistance to FDA reviewers overseeing medical software submissions and coordinate digital health initiatives across FDA. State laws also may be implicated with regard to how such technology is licensed or regulated under state public health, consumer protection, and medical practice licensure requirements.

Data Protection and Privacy Issues

In the United States, there is no single, comprehensive national law regulating the collection and use of personal data. When health information is concerned, the Health Insurance Portability and Accountability Act (HIPAA) will be a central compliance focus. A technology entity that provides services to a healthcare provider (HCP) and, in so doing, has access to patients' (or others') individually identifiable health information (protected health information or PHI) is a "business associate" who is regulated, along with the HCP, under the privacy, data security, and security breach notification rules implementing HIPAA. The HIPAA rules are detailed and somewhat complex. Notably, the rules require the creation of written policies and procedures and the implementation of training programs for employees, agents, and subcontractors with access to PHI.

HIPAA does not provide a private right of action, but rather provides for enforcement by the Department of Health and Human Services (HHS) and, in cases brought on behalf of citizens of a State, by the Attorney General of that State. Attorney General actions are extremely rare in the United States, but HHS has been increasing its enforcement efforts under HIPAA, including against HIPAA business associates. Most enforcement actions involve HIPAA Security Rule violations, and a finding of liability can subject a company to very substantial fines. HIPAA also contains a criminal liability provision, which is enforced by the Department of Justice (DOJ), but DOJ has been relatively limited in its HIPAA enforcement proceedings, seeking to prosecute only very egregious violations.

In addition to various bodies at the federal level, many states have sought to regulate the collection and use of personal data. The HIPAA rules do not preempt individual state or local laws governing health information privacy, security, or security breach notifications that are more protective of individuals' privacy. Accordingly, entities doing business in the United States that have access to patients' or others' PHI have significant liability risks that need to be carefully considered and mitigated through proactive privacy and data security measures.

Cybersecurity and Quality Control Implications

A corollary of the data privacy issues are the cybersecurity issues that may arise from the application of AI to medical technologies. FDA only requires manufacturers to report a small subset of actions taken to correct device cybersecurity vulnerabilities and exploits that may pose a risk to health.[38] Nevertheless, FDA has emphasized that manufacturers should monitor, identify, and address cybersecurity vulnerabilities and exploits as part of their post-market management of medical devices in recent guidance.[39] The FDA also has issued product-specific safety communications discussing cybersecurity vulnerabilities. On January 9, 2017, for example, FDA issued a Safety Communication confirming vulnerabilities in St. Jude Medical's implantable cardiac devices and Merlin@home Transmitter (a home monitor that wirelessly connects to the patient's implanted cardiac device and reads the data stored on the device to enable remote care management of patients).[40]

In addition, the FDA Guidance on quality systems for software should be considered. Companies that make and market medical devices must have a comprehensive system to ensure product safety and quality.[41] Medical device software products are subject to design control provisions.[42] These regulations require design input requirements to be documented, and that specified requirements be verified. According to the FDA, software verification "looks for consistency, completeness, and correctness of the software and its supporting documentation, as it is being developed, and provides support for a subsequent conclusion that software is validated.[43]

Conclusion

The Association of the British Pharmaceutical Industry, which represents research-based biopharmaceutical companies in the United Kingdom, recently stated that it anticipates more extensive use of machine learning or AI being applied in the sector.[44] This prediction will become a reality if the current flurry of industry initiatives based on AI continues to grow, and business decisions should take account of the evolving regulatory requirements. In the EU, AI software properly classified as a medical device must comply with the rules seeking to establish its safety and performance. The new EU Regulations adopted on April 5, 2017, which come into effect on May 26, 2020, will widen the scope of the regulatory regime considerably. The regulatory regime will require all operators to re-assess product classification in view of the new requirements well in advance of this deadline to ensure business continuity once the new regime takes effect. Given the capability of AI to capture various forms of personal data, cybersecurity will become very important to ensure sustainability of the technology, including periodic review of the internal processes to take full account of the requirements of the over-hauled EU rules governing processing of personal data.

In the United States, a variety of legal, regulatory, and compliance issues may arise for AI developers based on the intended use of the product. Once a product is classified as a medical device, its class will define the applicable regulatory requirements, including the type of premarketing notification/ application that is required for FDA clearance or approval. Regardless of the product's classification, however, AI developers will need to assess whether the HIPAA rules apply and any design controls and post-manufacture auditing that also may apply in the cybersecurity space.

Notes

1. Jackie Hunter, "How artificial intelligence is the future of pharma," *Drug Target Review*, December 5, 2016: *https://www.drugtargetreview.com/news/15400/artificial-intelligence-drug-discovery*.
2. Williams, K. and Bilsland, E. *et al*., "Cheaper faster drug development validated by the repositioning of drugs against neglected tropical diseases," *Interface*, Feb. 4, 2015.
3. Joao Medeiros, "The startup fighting cancer with AI," *WIRED*, March 22, 2016: *http://www.wired.co.uk/article/ai-cancer-drugs-berg-pharma-startup*.
4. Sanford Medicines News "Researchers design more accurate method of determining premature infants' risk of illness," Sept. 8, 2010: *https://med.stanford.edu/news/all-news/2010/09/researchers-design-more-accurate-method-of-determining-premature-infants-risk-of-illness.html*.
5. Houston Methodist, "Artificial intelligence expedites breast cancer risk prediction," August 29, 2016: *http://www.houstonmethodist.org/1285_houstonmethodist/1315_newsroom/1316_newsroom_newsandevents/newsdetail/?key={0370A9DC-5D5E-41B0-A4DB-97F3F519BEC9}*.
6. IEEE Spectrum, "IBM Watson Takes on the Genetics of Brain Cancer," March 19, 2014: *http://spectrum.ieee.org/tech-talk/biomedical/diagnostics/ibm-watson-takes-on-brain-cancer*.
7. Medtronic News, "IBM and Medtronic to Partner to Improve Diabetes Care," April 13, 2015: *http://newsroom.medtronic.com/phoenix.zhtml?c=251324&p=irol-newsArticle &ID=2034597*.
8. Johnson & Johnson News, "Johnson & Johnson and IBM Announce Plans to Collaborate on Advanced Solutions Designed to Transform Healthcare Delivery," April 13, 2015: *https://www.jnj.com/media-center/press-releases/johnson-johnson-and-ibm-announce-plans-to-collaborate-on-advanced-solutions-designed-to-transform-healthcare-delivery*.
9. IBM News, "Novo Nordisk and IBM partner to build diabetes care solutions on the Watson Health Cloud," Dec. 10, 2015: *https://www-03.ibm.com/press/us/en/pressrelease/48316.wss*.
10. Shire, "Specialty biopharmaceutical company reaps data analysis and process efficiencies," March 2017: *http://statistica.io/wordpress/wp-content/uploads/shire-specialty-biopharmaceutical-company-reaps-data-analysis-and-process-efficiencies-case-study.pdf*.
11. EMB News, "Celgene and IBM Watson Health Forge Collaboration Designed to Transform Patient Safety Monitoring," Nov. 1, 2016: *http://www-03.ibm.com/press/us/en/pressrelease/50927.wss*.
12. IBM News," The Weather Company Announces Watson Ads, To Humanize The Ad Experience for Consumers with Industry-First Capability," June 2, 2016: *https://www-03.ibm.com/press/us/en/pressrelease/49858.wss*.

13. IBM News, "New Cold and Flu Tracker from The Weather Company, an IBM Business, Provides Consumers with Real-Time Updates of Flu Activity at a Hyper-Local Level," Oct. 6, 2016: *https://www-03.ibm.com/press/us/en/pressrelease/50730.wss*.

14. Directive. 93/42/EEC of June 14, 1993, concerning medical devices (as amended). The Directive will be replaced by Regulation (EU) 2017/745 following its adoption on April 5, 2017.

15. *See e.g.*, Case C-140/07 *Hecht-Pharma*, Case C-27/08 *BIOS Naturproductke*, as confirmed by C-308/11 *Chemische Fabrik Kreussler*.

16. Case C-27/08 BIOS *Naturproductke*.

17. Guidelines on the Qualification and Classification of Stand Alone Software used in Healthcare within the Regulatory Framework of Medical Devices, MEDDEV 2.1/6, July 2016.

18. C-329/16 – SNITEM (Syndicat national de l'industrie des technologies médicales) and Philips France, 28 June 2017.

19. European Commission, "Report of the Working Group on mHealth assessment guidelines," June 9, 2017: *https://ec.europa.eu/digital-single-market/en/news/report-working-group-mhealth-assessmtent-guidelines*.

20. Regulation (EU) 2017/745 of the European Parliament and of the Council of April 5, 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

21. Regulation (EU) 2016/679.

22. Article 5(2) of the GDPR.

23. Article 30(1)(b) of the GDPR.

24. Article 32(1) of the GDPR.

25. The provision of informed consent is addressed by Articles 6(1) and 7 of the GDPR.

26. Recital 71 and Article 13 of the GDPR.

27. Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6, 2016 concerning measures for a high common level of security of network and information systems across the Union.

28. Federal Food, Drug and Cosmetic Act 21 U.S.C. § 321(h).

29. Preamble to Final Rule on Intended Uses, 82 Fed. Reg. 2193 (Jan. 9, 2017).

30. FDA, Guidance for Industry and Food and Drug Administration Staff: Mobile Medical Applications (Feb. 2015), available at *https://www.fda.gov/downloads/MedicalDevices/.../UCM:263366.pdf.*

31. 21 C.F.R. § 880.6310.

32. FDA, Guidance for Industry and Food and Drug Administration Staff: Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices (Feb. 2015), available at *https://www.fda.gov/downloads/medicaldevices/deviceregulationand guidance/guidancedocuments/ucm401996.pdf.*

33. FDA, Draft Guidance: Software as a Medical Device (SAMD): Clinical Evaluation (Aug. 2016), available at *https://www.fda.gov /downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM524904.pdf.*

34. 21st Century Cures Act, Pub. L. No. 114 – 255 § 360.

35. *Id.*

36. *Id.*

37. Jeremy Hsu, "FDA Assembles Team to Oversee AI Revolution in Health," *IEEE Spectrum*, May 29, 2017: *https://spectrum-ieee-org.cdn.ampproject.org/c/spectrum.ieee.org/the-human-os/biomedical/devices/fda-assembles-team-to-oversee-ai-revolution-in-health.amp.html*; Megan Molteni, "Medicine is going Digital. The FDA is Racing to Catch Up," *Wired* (May 22, 2017), *https://www.wired.com/2017/05/medicine-going-digital-fda-racing-catch/*.

38. *See* 21 C.F.R. Part 806.

39. FDA, Guidance for Industry and Food and Drug Administration Staff: Postmarket Management of Cybersecurity in Medical Devices (Dec. 2016), available at *https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf.*

40. FDA Safety Communication, Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter (Jan. 2017), available at *https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm.*

41. *See* 21 C.F.R. Part 820.

42. *See* 21 C.F.R. 820.30.

43. FDA, Guidance for Industry and Food and Drug Administration Staff: General Principles of Software Validation (Jan. 2002), available at *https://www.fda.gov/RegulatoryInformation/Guidances/ucm085281.htm.*

44. ABPI, A perspective on machine learning in the pharmaceutical industry (Mar. 2017), available at *http://www.abpi.org.uk/our-work/library/industry/Documents/A_perspective_on_ma chine_learning_in_the _pharmaceutical_industry.pdf*.