Regulatory considerations for cybersecurity and data privacy in digital health and medical applications and products

Proliferation of products, applications and services that collect personal and health-related information is giving rise to a new set of regulatory rules and requirements

Svetlana Lyapustina, PhD and Katherine Armstrong, JD
Drinker Biddle & Reath, LLP

Abstract

In an effort to improve patient adherence with inhalation therapies, many companies are developing mobile applications, devices or add-ons that enable electronic interactions with the user, such as monitoring, reminders, training and health alerts. These technological innovations hold the promise of improved healthcare outcomes, but they bring with them a new host of regulatory and legal considerations. Companies face a challenge, therefore, of maximizing their data assets while minimizing their legal and regulatory risks against the backdrop of a complex web of laws and regulations around the world. This article provides an overview of this rapidly evolving landscape as well as some guiding principles that can help companies in their digital-product development.

Introduction

Opportunities

A recent survey indicates that 46 percent of American consumers are now considered active digital-health adopters, having used digital-health tools such as wearable devices or telemedicine.[1] Almost every week, trade news outlets and even mainstream media publish reports of new "digital," "e-connected," "bluetooth" or "smart" medical devices, platforms or add-ons. Sensor-enabled and internet-connected products are hailed as game-changers because they may enable patients to engage more directly in their own healthcare, or at least health monitoring. They can also provide researchers or physicians with real-time data and make it easier for them to both find and monitor those enrolled. For instance, Apple is now conducting a study with Stanford Medical, in which study participants will download the Apple Heart Study App, and the Apple Watch's heart rate sensor will collect data on irregular heart rhythms and receive a notification if irregular heart rhythms are identified.[2] As another illustration, the United States Food and Drug Administration (FDA) recently approved a pill that digitally tracks whether patients have taken their medication. This is the first drug in the US with a digital ingestion tracking system.[3]

Similar digitalization of medical treatments and patient-related information is occurring in many other areas of healthcare and clinical research. For example, real-time patient data from medical devices and wearables can be used in the context of clinical trials, adverse event reporting, monitoring of adherence or in emergency room settings where the device can pinpoint, with high precision, the time and other circumstances of the onset of a given medical emergency. Physicians and hospitals are switching to electronic health records and rely on cloud-stored information to track individual patients or to make diagnoses. At an even higher level in the healthcare system, comprehensive databases of medical insurance claims contain a wealth of information about patients' insurance, financial details, enrollment data, demographics, diagnoses, procedures, hospitalizations and medications dispensed.

Respiratory conditions are among those that have been recognized as standing to benefit from digital-health tools through improved patient care and healthcare utilization.[4] Indeed, many examples of new technologies are intended for use with inhalation therapies. Several types of connected inhalers are already on the market and many more are in development.[5] These technolo-

Table 1

Some Examples of Functionalities Offered by "Smart" Inhalers and Add-ons

Domain	Examples
Device performance	• Dose counting • End-of-unit digital indicator • Coordination of actuation with the patient's breathing • Step-by-step instructions in real time on the use of the device
Patient's behavior and health status	• Reminder to take a dose • Record of patient's use information and sharing it with third parties (e.g., health-care provider) • Record of exact time and GPS location of a patient's symptoms exacerbation, and sharing these data with third parties
Education and general information	• Local alerts, such as high pollen count and pollution • Training resources (visual aids, videos, online chats with trained staff) • Community support (e.g., emailed newsletters, information about local meetings) • Announcements of relevant products and service information

gies (see Table 1) offer varying functionalities, ranging from simple dose counting and local weather alerts, to mobile apps reminding patients to take their medication or tracking their asthma triggers. Moreover, inhalers with GPS sensors or wearable devices are able to provide the exact time and GPS location of a patient's asthma attack.

Concerns

In step with all these technological developments, society's sensitivity to the ownership of patients' data is also rising; just as the role of patients as the rightful focus and center of any medical program or product development is coming to the forefront of public's consciousness.[6-9] This drive towards patient-centric medicine may influence the interpretation of existing, and the emergence of new, regulatory and legal requirements related to "digital health." The concerns already raised at the federal level (in the US) and therefore the potential direction of future regulations can be surmised from the 2016 report by the US Department of Health and Human Services (HHS)[10] and the 2017 inter-agency report by the Task Force created by the US Congress.[11]

The current data explosion is manifested not only in the volume and scale of gathered and stored data, but also in the velocity with which these data move, the variety of data sources, the multitude of potential venues where such data may be used and the emerging tendency to combine information contained in various centralized databases. Taken together, all these data create a wonderful opportunity for optimizing treatments, improving adherence, minimizing medical errors, supporting healthy lifestyle choices and contributing to better health (see Table 2). Along with the benefits, however, come new challenges, such as potential increases in cost of treatments, fear of penalties for lack of adherence, additional burdens on the healthcare providers, potential misuse of the data and vulnerabilities to hacking and privacy breaches. Legislators and regulators are stepping up to address these latter concerns in particular.

A way forward

This article provides an overview of the current (as of the end of 2017) regulatory landscape in the areas of patient data privacy and medical device cybersecurity. The article's focus is on the United States (US) and European Union (EU), as these world regions have issued the most detailed requirements and expectations to date, although many other countries have, or are developing, their own laws in this field. In addition to government-issued rules and regulations, various standard-setting bodies publish technical guidelines that may be applicable to digital products in general, including in a healthcare setting (e.g., the International Organization for Standardization, the Institute of Electrical and Electronic Engineers (IEEE), the International Electrotechnical Commission and others). Note that the title of a standard need not include the words "digital" or "cybersecurity" to be applicable in this field. For example, standard ISO 13485, focused on Quality Management Systems,[12] expands the concept of risk management, which may be interpreted as including risks related to cybersecurity. Compliance with the ISO, IEEE and other international standards may be optional or mandatory, depending on the jurisdiction.

Table 2

Some Pros and Cons of Interconnected Devices

Examples of Benefits	Examples of Concerns
Patient receives information that may help improve patient's technique or consistency using the device, leading to better drug delivery and, consequently, to better health outcome.	Patient's concerns: • Will my treatment cost more? • Is the device too complicated to use? • Will the device work if the battery runs out? • Will my insurance pay for the device or will my rate increase if I don't comply 100%? • Who will see my data and how will it be used?
Physician can review patient's use patterns and, if needed, initiate interventions to improve adherence, understand impediments to consistent compliance with the prescribed therapy, or change prescription.	Physician's concerns: • Data review and analysis requires time and specially trained staff. How will these increased demands be reimbursed? • What are my legal obligations and liabilities associated with collecting and using my patients' real-time data?
Regulators recognize potential benefits to the overall public health, such as potential improvement in patient compliance, on-site instructions enabling correct use, automatic alerts for help in case of life-threatening situations and others.	Regulators' concerns: • Will all patients sufficiently understand and correctly use the digital components? • Will the digital components perform as intended under real-use conditions, which may include low battery, intermittent internet connection, poor signal reception, high-temperature or high-humidity, interference from other devices? • Will the patient be able to receive medicine if the digital component fails for any reason? • Will the patient's health or care be endangered if the digital component is outdated, hacked, or otherwise compromised? • Will the patient data be appropriately protected?

Along with data privacy and cybersecurity issues, developers of digitally enhanced medical devices and mobile apps have to consider other regulatory and technical challenges, such as human factors studies, digital components' interoperability and manufacturability, and a system's reliability and robustness, to name a few. If digital components contribute to clinical diagnoses or decision making (e.g., creating a dosing plan), additional regulatory requirements will become relevant. These topics, however, are outside the scope of the current review. Specific regulatory guidance in these areas is currently lacking, but interested readers may consult published regulatory information (e.g., posted by the US Food and Drug Administration[13] and the European Medicines Agency[14]), and output from public conferences (e.g., RDD[15] and IPAC-RS/ISAM[16]).

In general, this field is evolving rapidly and along many dimensions simultaneously. Product developers would be wise to pay close attention to both the promises and potential pitfalls of new technologies.

Legal framework for data privacy and cybersecurity

In the US, the laws governing consumer data privacy at the federal level are segmented, and their application depends on the status of the entity involved, the types of data, the purposes for which data are used and, sometimes, the affected population. In addition, many states have their own privacy laws that extend beyond federal requirements. In contrast, the European Union approach is radically different, where individual privacy is a fundamental right.

Table 3

US Privacy Laws Addressing Potential Harmful Uses

Law's Focus	Example	US Federal Law
Industries	Healthcare Industry	Health Insurance Portability and Accountability Act (HIPAA)
Activities	Sending Spam	Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act
Individuals	Children	Children's Online Privacy Protection Act (COPPA)
Data Types	Consumer Report Information	Fair Credit Reporting Act

US federal laws

In the US, currently, there is no overarching privacy law applicable to all data processing activities. Rather, there are a variety of sector-specific laws that touch on privacy and data security. In addition to these laws, there are common-law privacy torts. Table 3 provides examples of federal laws that focus on specific types of data or protected populations.

The US Health Insurance Portability and Accountability Act (HIPAA) establishes national standards to protect individuals' medical records and other personal health information. It applies to *covered entities* and their business associates. Covered entities are defined in the statute to include (1) *health plans*—e.g., health insurance companies, HMOs, company health plans and government programs that pay for healthcare; (2) *healthcare clearing houses*—e.g., entities that process nonstandard health information they receive from another entity into a standard; and (3) *healthcare providers*—e.g., doctors, clinics and pharmacies, but only if they transmit any information in an electronic form in connection with a transaction for which the US Department of Health and Human Services has adopted a standard.[17]

The HIPAA Privacy Rule[18] requires appropriate safeguards to protect the privacy of personal health information and it sets limits and conditions on the users and disclosures that may be made of such information without patient authorization. The key type of information that HIPAA is designed to protect are *personal identifiable information* (PII), and, in particular, *personal identifiable health information* (PHI).[19] PII means any confidential or sensitive information that can be related back to an individual, such as their name, postal or email address, social security number or any *combination* of data that could be used to identify a person (e.g., a combination of birth date, zip code and gender). PHI can be thought of as PII connected to information about health status, provision of healthcare, or payment for healthcare linked to a specific individual.

Among other things, HIPAA requires covered entities and their business associates to take certain steps to secure and protect PHI, and also requires that reasonable efforts be taken to limit the uses and disclosure of PHI. HIPAA permits covered entities to use and disclose PHI for their own treatment, payment and healthcare operations purposes. Specific patient authorization is required, however, for use or disclosure of PHI for other purposes; and there are other federal laws that may apply.

Pharmaceutical and medical device companies are generally not covered entities under HIPAA (except in regard to the health benefits plans offered to employees). Nevertheless, such companies typically do engage in programs and activities that involve some use or disclosure of PHI by a covered entity or its business associates. Even if HIPAA does not apply directly, companies are encouraged to follow best practices to protect the privacy and security of the PHI in their possession. Therefore, drug or device manufacturers should use, whenever possible, de-identified information, which is not considered PHI. Non-compliance with HIPAA may have serious consequences. In the first five months of 2017 alone, nine legal cases were brought by the Health and Human Services Office for Civil Rights (OCR) for HIPAA violations, and many of these settlements required payments in the millions of dollars.

HIPAA is one, but not the only, law that may apply to entities operating in the US. Broadly speaking, in the US, processing of personal data is allowed unless it is prohibited. The US Federal Trade Commission (FTC) is the main regulator at the federal level enforcing data privacy and cybersecurity. This authority stems from Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices. "Deception" is a misrepresentation or omission or a broken promise.[20] "Unfairness" is an act or practice that is likely to cause significant injury, is not outweighed by countervailing benefits, and could not be reasonably avoidable.[21]

The FTC has brought more than 100 enforcement actions involving privacy and data security. The underlying violations included misrepresentations regarding privacy or data security, or inadequate data security which allowed, for example, identity thieves to access consumers' financial information. Unlike the OCR, Section 5 does not provide for monetary relief. Instead, the FTC's settlements result in injunctive relief and a

Table 4

A Sampling of FDA Guidance Documents Related to Digital Elements in Medical Products

Year	Guidance
1999	*Off-The-Shelf Software Use in Medical Devices*
2002	*General Principles of Software Validation*
2005	*Content of Premarket Submissions for Software Contained in Medical Devices*
2014	*Distinguishing Medical Device Recalls from Medical Device Enhancements*
2015	*Mobile Medical Device Applications*
2015	*Medical Device Data Systems, Medical Image Storage Devices and Medical Image Communications Devices*
2016	*General Wellness: Policy for Low Risk Devices*
2016	*Software As A Medical Device (SAMD): Clinical Evaluation*
2016	*Medical Device Accessories – Describing Accessories and Classification Pathway for New Accessory Types*
2016	*Postmarket Management of Cybersecurity in Medical Devices*
2017	*Qualification of Medical Device Development Tools*
2017	*Manufacturers Sharing Patient Specific Information from Medical Devices with Patients Upon Request*
2017	*Use of Real-World Evidence to Support Regulatory Decision-Making for Medical Devices*
2017	*Design Considerations and Premarket Submission Recommendations for Interoperable Medical Devices*
2017	*Deciding When to Submit a 510(k) for a Change to an Existing Device*
2017	*Deciding When to Submit a 510(k) for a Software Change to an Existing Device*

requirement that a company establish appropriate privacy and data security processes.

US state laws and regulatory guidance

Many of the US states have laws related to data privacy. As of mid-2017, five states were actively drafting bills on biometrics—which are distinctive characteristics that can be used to identify an individual, such as fingerprints, facial features, DNA, eye or iris recognition or voice recognition.

Another example of state activities in this area is breach notification laws. HIPAA does have specific requirements that include notification to the OCR, and in some cases to the individual(s) affected, if certain PHI has been breached; but there is otherwise no federal breach notification law. However, 48 of the 50 US states, as well as the District of Columbia, Guam, Puerto Rico and the Virgin Islands, all have breach notification laws that require private or governmental entities to notify individuals of security breaches of information involving personally identifiable information. Security breach laws typically have provisions regarding:

- Who must comply with the law, the definitions of "personal information" (e.g., name combined with social security number, drivers licenses, or state identification cards, or health or financial information);
- What constitutes a breach (e.g., unauthorized acquisition of the data);
- Requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., encrypted information).

This seemingly simple action—notification about a breach—can very quickly become a very complex task. If the notification requirement is indeed triggered, the organization responsible will have to identify all applicable laws in all pertinent jurisdictions, and then find a way to contact each of the affected individuals.

FDA guidance for industry

To minimize risk of a breach, any company that collects and uses personal information should monitor, identify, and address cybersecurity vulnerabilities that may exist in their organization. To assist industry, the FDA issued a final guidance on post-market management of cybersecurity.[22] This and other relevant guidances from the FDA that may be of interest to developers of digital health products are listed in Table 4. These regulatory documents are not legally binding but they do lay out expectations of the agency responsible for granting marketing approvals. Tellingly, there has been a surge in the number and range of guidances on the topics related to digital products in the last several years. This trend is likely to continue.

In the US, applications for products intended for respiratory delivery are typically reviewed by the FDA Center for Drugs Evaluation and Research (CDER), but

other FDA centers may also be involved or at least consulted—especially the Center for Devices and Radiological Health (CDRH). For this reason, understanding requirements of all relevant centers is important, particularly since they may vary to some extent in details, terminology and general approaches.

For example, CDRH (but not CDER) has a formal program for recognizing certain standards issued by international organizations. In mid-2017, the FDA added "Standard for Software Cybersecurity Network-Connectable Products, Part I: General Requirements (UL 2900-1 Ed. 1 2017)" to their recognized standards.[23] A list of recognized standards and other guidances related to wireless medical devices is also maintained on the CDRH website.[24]

A forward-looking "Digital Health Innovation Action Plan"[25] has been articulated by the FDA Commissioner, confirming the high interest regulators are going to take in the digitally enhanced products. Regulatory considerations more specific for inhalation therapy products were presented at a 2017 public workshop, which discussed the FDA, industry and user perspectives.[26]

European laws and regulations

Global pharmaceutical companies have largely used the European Union (EU) privacy-protection requirements (which are typically stricter than those in the US) as a baseline, with some local variation for functions such as R&D and adverse event reporting. On May 25, 2018, the EU's new General Data Protection Regulation (GDPR) comes into effect.

GDPR applies to processing of *personal data* by a data controller or processor in the EU. *Personal data* is any information relating to an identified or identifiable natural person. GDPR will extend to all foreign companies processing data of EU residents.

Under GDPR, data subjects must receive notice about the collection and use of their data. All processing of personal data requires a legal justification. There are stricter requirements for processing of sensitive categories of personal data. Personal data can only be used for the purpose collected.

In addition, Privacy Impact Assessments are required for processing that is likely to result in high risk to data subjects. Controllers must implement technical and organizational measures to ensure that data protection principles are incorporated ("privacy-by-design").

GDPR also establishes requirements related to:

- Data protection officers;
- Recordkeeping;
- Reporting and consultation;
- Breach notification;
- Cross border data transfers;
- Liability and sanctions for noncompliance (which can be as high as $10 million or 2% of global revenue).

Looking into the near future, the secondary legislative acts and guidelines that are expected to come out over the next few years, and which are intended to clarify the implementation of the new European Medical Devices Regulation (MDR),[27] may touch upon issues relevant to digital and interconnected products, but those details remain to be seen. The MDR—which was adopted in May 2017—will completely replace the Medical Device Directives by 2020.[28]

European countries that are not members of the EU (such as Iceland, Norway, Switzerland, and soon the UK) may have their own approaches to protecting data privacy and cybersecurity, and otherwise regulating digital-health products. For example, in the UK, the National Health Service has launched an online library of mobile apps.[29] The registration process there includes a Digital Assessment Questionnaire, which gives some sense of the regulatory expectations in that region. It therefore would be prudent for developers to review all relevant laws in countries of interest before submitting a product dossier for marketing authorization.

Principles to follow

In general, monitoring the adoption of data privacy and data protection laws throughout the world is challenging. Nevertheless, as laws and regulations develop in this area, there are a few key principles that could be used to guide digital product development and to minimize regulatory or legal risks, namely: notice, choice, access and security (see Table 5). These and other relevant concepts are discussed in more detail in the "Technology Assessment: Internet of Things" report published in May 2017 by the US Government Accountability Office.[30]

Conclusion

Developers of smart inhalers and add-ons, including mobile applications and digital sensors, should keep in mind the following general concepts related to patient data privacy and cybersecurity: notice, choice, access and security.

Laws regulating these areas are proliferating at the state level (in the US) and country level (in the EU), in addition to more general applicable statutes at the Federal or Union level.

Staying abreast of the relevant legal and regulatory developments in this field is challenging but increasingly necessary as medical devices and services acquire new functions, capabilities and concomitant vulnerabilities.

Readers should also keep in mind that laws are continually evolving, and this article is meant only as a brief summary for general information. It is imperative that product developers consult with their own regulatory and legal advisers to review and apply the most current laws and regulations.

Table 5

Key Principles of Data Privacy

Principle	What It Means for Product Developer
Notice	Notify the user about the fact and purpose of data collection, as well as any subsequent deviations from the originally stated conditions of data use.
Choice	Give users a choice to opt-in or opt-out of participating in the data collection process.
Access	Provide users with a method to access data about themselves and to contest data's accuracy.
Security	Implement safeguards to prevent unauthorized or inappropriate use of data or disclosure of personal information.

References

1. HIT Consultant. 12 Reasons Why Digital Health Has Reached the Tipping Point in 2016. http://hitconsultant.net/2016/12/16/consumer-digital-health-adoption-report/.

2. Apple Heart Study Launches to Identify Irregular Heart Rhythms. November 2017. https://www.apple.com/newsroom/2017/11/apple-heart-study-launches-to-identify-irregular-heart-rhythms/.

3. FDA. News Release: FDA Approves Pill with Sensor that Digitally Tracks if Patients Have Ingested Their Medication. November 2017. https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm584933.htm.

4. The IQVIA Institute for Human Data Science. The Growing Value of Digital Health: Evidence and Impact on Human Health and the Healthcare System. November 2017. https://www.iqvia.com/institute/reports/the-growing-value-of-digital-health.

5. Smyth, H. New Delivery Technologies for Orally Inhaled Products. Presentation at IPAC-RS/ISAM Workshop, June 2017. Available at www.ipacrs.com.

6. Jarrett MP. JAMA. Cybersecurity-A Serious Patient Care Concern. 2017 October 10;318(14):1319-1320. doi: 10.1001/jama.2017.11986. https://jamanetwork.com/journals/jama/article-abstract/2654933.

7. Blau, M. An Expert Sounds the Alarm about Unchecked Sharing of Health App Data. STAT, October 26, 2017. https://www.statnews.com/2017/10/26/unchecked-sharing-health-app-data/?s_campaign=stat:rss&utm_source=STAT+Newsletters&utm_campaign=482648571b-STAT_Plus&utm_medium=email&utm_term=0_8cab1d7961-482648571b-149674889.

8. Kramer DB and Fu K. Cybersecurity Concerns and Medical Devices: Lessons from a Pacemaker Advisory. JAMA. 2017. doi:10.1001/jama.2017.15692.

9. Mikk KA, Sleeper HA and Topol EJ. The Pathway to Patient Data Ownership and Better Health. JAMA. 2017;318(15):1433-1434. doi:10.1001/jama.2017.12145.

10. DHHS. Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA 2016. https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

11. Health Care Industry Cybersecurity Task Force. Report on Improving Cybersecurity in the Health Care Industry. 2017. https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

12. International Organization for Standardization. ISO 13485:2016. Medical Devices—Quality Management Systems—Requirements for regulatory purposes. https://www.iso.org/standard/59752.html.

13. FDA maintains a webpage on Digital Health: https://www.fda.gov/medicaldevices/digitalhealth/.

14. EMA Workshop on "Big Data." Comprehensive report: http://www.ema.europa.eu/docs/en_GB/document_library/Report/2017/02/WC500221938.pdf.

15. Respiratory Drug Delivery (RDD) 2017. Podium presentations and vendor workshops on e-connected devices. www.rddonline.com.

16. "New Frontiers in Inhalation Technology," a 2017 Joint Workshop presented by the International Pharmaceutical Aerosol Consortium on Regulation and Science and the International Society for Aerosols in Medicine. Perspectives of academia, regulators and industry. www.ipacrs.org.

17. US Code of Federal Regulations. 45 C.F.R. § 106.103. See also https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

18. US Code of Federal Regulations. 45 C.F.R. Part 160.

19. US Code of Federal Regulations. 45 C.F.R. § 106.103.

20. United States Code. 15 U.S.C. § 45(a).

21. United States Code. 15 U.S.C. § 45(n).

22. United States Food and Drug Administartion. Guidance for Industry and Food and Drug Administration Staff. Postmarket Management of Cybersecurity in Medical Devices. 2016. https://www.fda.gov/down

loads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

23. Federal Register Volume 82, Number 160 (Monday, August 21, 2017)]. Pages 39591-39598. Notices. Department Of Health And Human Services. Food and Drug Administration, [Docket No. FDA-2004-N-0451]. Food and Drug Administration Modernization Act of 1997: Modifications to the List of Recognized Standards, Recognition List Number: 047. https://www.gpo.gov/fdsys/pkg/FR-2017-08-21/html/2017-17603.htm.

24. FDA, CDRH. Wireless Medical Devices. https://www.fda.gov/MedicalDevices/DigitalHealth/WirelessMedicalDevices/default.htm?elqTrackId=3126532500D31D75B186A0EF896E223A&elq=048e888a7be84bac9518340fa7e594c6&elqaid=1092&elqat=1&elqCampaignId=607#8.

25. FDA. Digital Health Innovation Actin Plan. 2017. https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM568735.pdf.

26. Highlights from the 2017 IPAC-RS/ISAM Joint Workshop "New Frontiers in Inhalation Technology" Smyth HD, Colthorpe P, George M, Jansen P, Fuglsang A, Armstrong KE and Lyapustina S. Journal of Aerosol Medicine and Pulmonary Drug Delivery. November 2017, ahead of print. https://doi.org/10.1089/jamp.2017.1425.

27. European Council. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 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. http://eur-lex.europa.eu/legal-content/ENG/TXT/PDF/?uri=CELEX:32017R0745&from=EN.

28. European Commission. The New Regulations on Medical Devices. https://ec.europa.eu/growth/sectors/medical-devices/regulatory-framework_en#new_regulations.

29. National Health Service (UK). Apps: Information for Developers. https://developer.nhs.uk/apps/.

30. US Government Accountability Office. GAO-17-75. Internet of Things. Available at https://www.gao.gov/assets/690/684590.pdf.

Katherine E. Armstrong, JD is counsel in Drinker, Biddle & Reath's Government & Regulatory Affairs Practice Group, Katherine.Armstrong@dbr.com, and Svetlana Lyapustina, PhD is senior director for science, regulation and policy within DBR's Pharmaceutical Consortia Management Group, svetlana.lyapustina@dbr.com. http://dbrondata.com.