nature electronics

PERSPECTIVE

https://doi.org/10.1038/s41928-019-0290-6

Ethical and legal issues of ingestible electronic sensors

Sara Gerke[1*], Timo Minssen[2], Helen Yu[2] and I. Glenn Cohen[3]

Ingestible electronic sensors are a promising technology for improving health outcomes that may, for example, be useful in monitoring and promoting the taking of medication. However, these sensors also raise ethical and legal challenges that need to be considered by all stakeholders—notably, the creators of such products—at the earliest stages of the development process. Here, we examine selected ethical and legal issues related to ingestible electronic sensors. We first briefly describe sensors that are already available on the US and European markets as well as potential future sensor combinations. We then focus on ethical aspects, discussing patient, provider, and social issues. Finally, we provide a comparative analysis of legal regulation of ingestible electronic sensors in the US and Europe.

In discussions on the cutting edge of medicine, few topics have drawn as much attention as digital health. The US Food and Drug Administration (FDA) defines the term broadly to everything from mobile health and health information technology to wireless medical devices and mobile medical apps to telehealth and precision medicine[1]. The European Commission refers to digital health and care as "tools and services that use information and communication technologies to improve prevention, diagnosis, treatment, monitoring and management of health and lifestyle"[2].

One sub-category of digital health that has recently made it to market is ingestible electronic sensors (IESs). An IES is usually either co-ingested with medicine or taken as an embedded part of a drug. Once ingested into the human body, it can communicate with a wearable sensor capable of detecting and recording data such as time of medication intake or behavioural and physiological metrics. The wearable sensor then forwards the collected information to a compatible computing device such as a smartphone or tablet computer, which then processes and displays the data. The display function can also be connected with a cloud database that enables data sharing, such as to a family member or physician.

Despite their vast potential to improve health outcomes (for example, by potentially facilitating monitoring and promoting adherence), IESs also raise ethical and legal challenges. In this Perspective, we first briefly describe IESs that are already available on the US and European markets as well as potential future IES combinations. We then focus on ethical aspects, discussing patient, provider, and social issues. This is followed by a comparative analysis of legal regulation of IESs in the US and Europe. Though highly promising, stakeholders, especially the creators of IESs, must remain attuned to the legal and ethical challenges.

IESs and future combinations

IESs are already available on the US and European markets. For example, Proteus Digital Health developed—independently of medication—a wearable sensor (also called a Patch) that records metrics such as heart rate, activity, and body position as well as time-stamped, patient-logged events usually generated when the patient marks an event by swallowing a grain-of-sand sized IES[3]. The IES activates once it reaches the stomach and communicates to the Patch worn on the skin[4]. The Patch collects the data and wirelessly sends it to a mobile computing device[3]. The compatible software arranges and displays ingestion events[3]. The system also enables the patient to share the information with a physician[4]. When the IES is co-ingested with medicine, the hope is it will help improve medication adherence. Proteus's wearable sensor, including the IES, has been CE-marked in Europe since 2010[4,5] and FDA-cleared since 2012[6]. A CE marking is a legal prerequisite to place a device on the market within Europe[7].

In 2017, Otsuka Pharmaceutical received New Drug Application (NDA) approval by FDA to market Abilify MyCite, a drug–device combination product of Proteus's IES and Otsuka's Abilify (that is, aripiprazole, a drug that is used to treat adults for schizophrenia, bipolar I disorder, and major depressive disorder)[8–10]. In this product, the IES is not physically separated from the active pharmaceutical product, but the drug tablet is embedded with the IES[8]. The Abilify MyCite system consists of four components: Abilify MyCite (that is, aripiprazole tablets with an IES); MyCite Patch (that is, Proteus's wearable sensor); MyCite App (that is, a smartphone application); and web-based dashboards for health-care providers[8]. This system has been developed to help patients with serious mental illness to facilitate a more open dialogue with their health-care team by allowing them to record their daily medication intake and access information about their objective medication ingestion, activity level as well as self-reported mood and rest[8]. Patients can also choose through the MyCite App to share this information with selected members of their care team and family with the hope it will improve adherence[8].

Abilify MyCite, as the first 'digital pill' approved by FDA, is just the first of a number of new IES products. For example, Proteus, Fairview Health Services, and University of Minnesota Health have just announced the first 'digital oncology pill' consisting of Proteus's IES and the chemotherapy medication capecitabine to help treat stage three and four colorectal cancer patients[11]. Researchers at the RMIT University in Melbourne, Australia, and others have recently published a human pilot study with an IES in the form of a capsule that can sense different gases in the gut such as oxygen, carbon

[1]Project on Precision Medicine, Artificial Intelligence, and the Law, Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics at Harvard Law School, Harvard University, Cambridge, MA, USA. [2]Centre for Advanced Studies in Biomedical Innovation Law, University of Copenhagen, Copenhagen, Denmark. [3]Harvard Law School, Harvard University, Cambridge, MA, USA. *e-mail: sgerke@law.harvard.edu

dioxide, and hydrogen[12]. This gas capsule offers a potential diagnostic tool for several disorders of the gut such as irritable bowel syndrome, and the researchers intend to commercialize the technology through a newly created company, Atmo Biosciences, in the future[12,13]. Scientists at the Massachusetts Institute of Technology (MIT) in Cambridge, USA, have developed a 'bio' IES combination product consisting of engineered probiotic sensor bacteria and ultra-low-power microelectronics packed in a single capsule that can detect gastrointestinal bleeding in vivo and enables new opportunities for improving the management and diagnosis of disease[14]. The use of IESs also holds promise for the treatment of drug-resistant tuberculosis since the current therapy usually relies on direct observations and has shown to be poorly implemented[15]. IESs could help health-care providers to identify patients that do not take their medication as prescribed and thus better focus their efforts on these patients as well as reduce financial charges on patients from repeated visits to health-care facilities[15]. Moreover, IESs may have great potential to improve adherence to pre-exposure prophylaxis, a daily drug for the prevention of HIV transmission[16].

Ethical challenges for IESs

IESs hold great potential to transform health care for the better. However, at the same time, they also create ethical challenges that stakeholders (for example, researchers, engineers, health-care providers, patients, ethicists, and regulatory authorities) need to be aware of and address in a collaborative effort as early as possible in the development process of these products. One of us (I.G.C.) has written about these issues in detail elsewhere[17], and thus here we summarize the relevant points and tailor them to IESs. It is helpful to group the issues into three categories: patient, provider, and social issues.

First, IESs raise a variety of patient issues—especially the ethical issues of autonomy and informed consent[17]. Because IESs will, at least initially, involve therapies with elements that are unfamiliar to patients, it is particularly important to ensure full voluntary and informed consent. However, the software component of IES products are distinct and will mean that at least part of the system (for example, use of the app) will involve user agreements, which many patients have trouble understanding and also most users routinely ignore[17,18]. It is unclear whether the click-through user agreement can partially or fully substitute for informed consent. That this software will likely have frequent updates raises additional challenges—patients may not understand what changes the update implements nor that future use may be conditional on accepting changes to the terms of use that go along with updates. Is it a sufficient response that the patient will fairly quickly excrete the IES and can choose not to resume usage in such an eventuality?

Ownership of the data collected by IES products raises a multitude of issues, including the question of the doctor–patient privilege and the related issue of medical confidentiality. The availability of this data in the hands of third parties might have implications on life insurance premiums, employment opportunities, and even personal relationships, depending on the national law of the country where the patient resides. IES makers must be frank about the future use of the collected data and the terms surrounding it[17]. For example, in what way will identified and de-identified data be stored and aggregated? With whom will it be shared? Can patients request that their data be destroyed and do such withdrawal rights apply to data that has already been analysed in aggregate form? To what extent do such rights of withdrawal conflict with potential requirements of post-market surveillance that may be imposed by FDA and other regulators? Finally, obtaining informed consent can be particularly challenging in cases of vulnerable patient groups such as prisoners, or individuals out on probation. When IESs will be used in such contexts, particular care must be taken to make sure the consent is not only informed but also voluntary[19].

A different patient-centred set of challenges pertain to data management and control, confidentiality, and privacy. Because IES products collect patient data, it is optimal to design them to enable patients to approve who (if anyone) has access to such data beyond the IES maker[17]. The more individuals are authorized to access the data, the more complicated the issues can become. Suppose that a patient decides to share the data with their families and friends: should those family members and friends be subject to duties of confidentiality similar to those of the clinicians[17]? Unlike the physician, whose duty of confidentiality is typically set out by governing statutes or case law, it seems much less likely that family or friends will have legally enforceable obligations in this context. Can ethics advice really adequately manage these kinds of familial relationships, or is each family and circumstance so distinct that generalized advice will be failing? The ability for patients to 'de-authorize' family members from receiving data is a partial salve, but such moves may also prompt concern and conflict, issues patients should be made aware of at the start of the process.

A final set of patient-centred ethical issues concern patient expectations. An IES may enable but not mandate a member of the patient's care team to access information such as ingestion to determine if the patient has or has not been taking their medication. Patients using an IES may have a different expectation as to whether or how often they are being 'checked up on'. Some thought has to be given to how to enable the care team and the patient to have a better 'meeting of the minds' on these issues such that patients' expectations better meet the reality of the care team's behaviour[17].

Second, IESs also raise provider-centred ethical issues. On the one hand, the hope is that IESs will improve the clinician–patient relationship by enabling the clinician to better understand what is going on (biologically and/or socially) with the patient, and thus facilitate a more open dialogue between both parties[8]. However, there will also be patients who may feel 'surveilled'—in the sense of unwanted observation—by their health-care providers through such systems. When a patient is the one who requests an IES as opposed to the non-IES formulation of the same therapy the voluntariness of the decision is at its zenith. In other cases, the pressure may be subtle or gross. Consider a patient who uses the IES formulation to please his or her family or a patient whose insurer will only cover the IES formulation. These are not easy waters to navigate, but effective use of IES products is built on a trusting doctor–patient relationship, where open dialogue is fostered and not chilled[17].

While IES systems are designed to primarily gather data on the patient, few physicians will realize at first how much information about the physician or other members of the care team (for example, tracking when a physician logs on) is also collected[17,18]. To what extent do members of the care team have to consent to the collection and use of their data? Does it matter whether the data is used by the maker of the IES to improve the system or by a private or public insurer to evaluate whether to authorize payment for the use of the IES by a particular physician or care team? Medical malpractice liability in the course of treatment with IESs is a real possibility, as it is with any other therapy. In both civil and indeed criminal litigation parties may seek to access information about the IES use—for example, after an adverse event the plaintiff's lawyer may want to determine whether the care team was checking the results of the IES, how often, and what they did or did not undertake to do based on such results[17,18]. The makers of IESs will need to plan ahead for how they will respond to requests for data in civil and criminal cases.

Third, IESs raise ethical issues beyond the patient–care team dyad. Should an IES provide a major benefit over existing therapies, how equitable will access to the technology be[17]? After all, IES products are likely to be more expensive than comparable non-IES versions, especially when the non-IES version is past its market exclusivity (that is, it is available as a generic)[17,20]. Will public or private insurers pay for the IES? They will quite sensibly want

proof that the patient is using the product and that it is providing enough additional benefit to the patient to justify the costs[17]. If the IES requires the use of a smartphone or other device as a prerequisite to use, to what extent will disparities in access to those technologies lead to disparities in IES access[17,21]? Finally, to secure public trust in IES products, transparency about all relevant aspects of such products is needed (for example, IES makers should be proactively reporting security breaches, including ransomware attacks)[17].

Legal regulation of IESs

With regard to legal regulation of IESs in the US and Europe, we should distinguish two different cases: first, an IES that is co-ingested with medicine and, second, an IES that is embedded as part of the drug itself.

Wearable sensors including IESs by themselves are medical devices in the US and Europe. In the US, a medical device is defined in section 201(h) of the Federal Food, Drug, and Cosmetic Act and ranges from a simple tongue depressor to a complex robotically assisted surgical device to an in vitro diagnostic product such as a test kit or reagent[22,23]. In particular, a medical device—in contrast to a typical drug—"does not achieve its primary intended purposes through chemical action … and … is not dependent upon being metabolized for the achievement of its primary intended purposes"[24].

FDA regulates medical devices intended for human use in the US and divides them into three classes: Class I (that is, low-risk devices such as patient scales), Class II (that is, moderate-risk devices such as sickle-cell test kits), and Class III (that is, high-risk devices such as replacement heart valves)[25]. New devices are automatically placed in Class III[26,27]. However, the 'De Novo' classification process offers sponsors the opportunity to request a risk-based evaluation by FDA for classification of their new devices into Class I or II[27,28].

In 2012, FDA classified Proteus's wearable sensor, including the IES, through the De Novo classification process into Class II under the generic name "Ingestible Event Marker"[6,29]. FDA also concluded that devices "substantially equivalent" to the Proteus device are classified as Class II under this generic name[6]. FDA clarified that this device type is not exempt from the premarket notification requirements of the Federal Food, Drug, and Cosmetic Act[6]. Thus, sponsors who intend to market this device type need to submit a Premarket Notification 510(k) before marketing the device and receive 'clearance' to market from the agency[6,30]. In contrast to Class III devices that require pre-market approval to provide reasonable assurance of their safety and effectiveness, Class II devices are 'only' subject to general controls and special controls[25]. General controls, for example, include requirements for establishment registration and medical device listing[31]. Special controls for Ingestible Event Markers such as Proteus's wearable sensor, including the IES, for example, consist of the following four measures: biocompatibility and toxicology testing; non-clinical, animal, and clinical testing; electromagnetic compatibility, wireless, and electrical safety testing; and special labelling such as the maximum number of daily device ingestions[29]. In addition, Proteus's device and substantially equivalent devices are prescription devices[29,32].

For cases such as Abilify MyCite where a drug product is physically embedded with an IES, the regulatory regime is somewhat different. In this instance, it is a combination product as defined in section 3.2(e)(1) of Title 21 of the Code of Federal Regulations, comprising of two components, namely a drug and a device, "that are physically, chemically, or otherwise combined or mixed and produced as a single entity." Marketing applications for combination products are typically based on their primary mode of action (PMOA)[33]. Abilify MyCite, for example, has a drug PMOA, thus requiring NDA approval. Abilify MyCite is also a prescription drug[10]. In contrast, the newly announced digital oncology pill by Proteus, Fairview Health Services, and University of Minnesota Health did not need to be approved by FDA since the drug capecitabine and Proteus's IES are only "loosely packaged" within a capsule[34]. However, Proteus intends to physically embed capecitabine with its sensor and then seek FDA approval for such a combination product[34].

Proteus and Otsuka had to work closely with FDA to figure out the kind of data needed for submission[35]. The next generation of digital health products should have an easier entry to the US market, both because the relevant pathways have been used and because FDA has announced a new Digital Health Innovation Action Plan that strives to ensure "timely access to high-quality, safe and effective digital health products"[36]. In particular, in November 2018, FDA proposed for public comment a framework for regulating prescription drug-use-related software (PDURS)—that is "software disseminated by or on behalf of a drug sponsor that accompanies one or more of the sponsor's prescription drugs", such as the MyCite App[37]. This framework does not focus on whether software is a device, and indeed applies irrespective of whether or not it is a device[37]. Instead, the focus of the proposed framework is on the output of PDURS that is presented to the end user (such as the displayed information on drug ingestion for the patient and patient-selected healthcare providers and caregivers in the case of IES systems such as the MyCite App)[37].

FDA takes a risk-based approach in its proposal[37]. The agency anticipates that in the majority of cases, the output of PDURS would be considered 'promotional drug labelling' and therefore would simply require submission of promotional materials (for example, screenshots of what the user will experience) at the time of initial dissemination, rather than approval by FDA[37].

In two situations, however, the agency has indicated that information about the output of PDURS may be included in 'FDA-required drug labelling' (that is, labelling that is approved by the agency)[37]. First, where there is substantial evidence demonstrated by the drug sponsor that the use of the PDURS results in a clinically meaningful improvement compared to its non-use[37]. Second, cases such as Abilify MyCite where there is a drug-led, drug–device combination product of which the PDURS is (an element of) a device constituent part[37]. For this second situation to apply, the PDURS also needs to provide essential information or function for the intended use(s) of such combination product[37]. To illustrate with the MyCite App as an example: because it is essential for the system to work to allow the patient—and with the patient's consent, the doctor—to review their drug ingestion data collected by the MyCite Patch, this function is essential to one of the intended uses of the combination product (that is, tracking drug ingestion)[37]. Consequently, information about this essential function of the MyCite App has to be included in FDA-required drug labelling under the new proposed framework (it was provided in actuality for this app)[37]. With regard to other software functions that are not essential for the use of the combination product (for example, the MyCite App's functions to self-report mood and rest), FDA may require a sponsor to disclose that those functions have not been approved by the agency[37]. FDA is currently seeking comments on its proposal from stakeholders before issuing draft guidance[37].

Importantly, FDA flags another situation as meriting a different regulatory approach: that is, "prescription drug-use-related software output may increase the potential for harm to health where it provides recommendations that may direct patients to make decisions about their drug or disease that would normally be made in consultation with a healthcare provider." In such cases, FDA indicates that "such software might be considered a device if it provides recommendations to patients to prevent, diagnose, or treat a disease or condition"[37].

In the EU, the Medical Device Directive 93/42/EEC (MDD)[38] applies to medical devices. A directive, in comparison to a regulation, needs to be transposed into national law[39]. On 25 May 2017, the new EU Medical Device Regulation 2017/745 (MDR)[40] entered into force[41]. However, with few exceptions, the MDR will only apply

in each member state from 26 May 2020 and repeal the MDD and the Active Implantable Medical Devices Directive 90/385/EEC (AIMD)[42,43]. In addition, at the same time as the MDR, the EU In Vitro Diagnostic Medical Devices Regulation 2017/746 (IVDR)[44] came into force[45]. The IVDR will generally apply two years later than the MDR (that is, from 26 May 2022) and repeal, inter alia, the In Vitro Diagnostic Medical Devices Directive 98/79/EC (IVDD)[46,47].

In principle, the current EU regulatory framework for medical devices therefore consists of three directives (until the MDR and IVDR come into force): AIMD, for active implantable medical devices such as pacemakers; IVDD, for in vitro diagnostics such as pregnancy tests; and MDD, for all other medical devices such as simple tongue depressors.

Medical devices may only be placed on the market in Europe if they fulfil all CE-marking requirements set out in the relevant directives. A medical device is defined in article 1(2)(a) of the MDD, IVDD, and AIMD, and similar to US law "does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means." Thus, in contrast to a medicinal product, as defined in article 1(2) of the Medicines Directive 2001/83/EC[48], a medical device typically acts by physical means. For example, smartphone apps may be classified as medical devices under certain conditions, such as where the software is "intended by the manufacturer to be used for human beings for the purpose of diagnosis, prevention, monitoring, treatment or alleviation of disease ... [or] … an injury or handicap"[49].

Similar to US law, medical devices according to the MDD are classified into product classes. In total, there are four classes of medical devices (instead of three classes in US law), taking into account their potential risks: Class I (low risk), Class IIa (medium risk), Class IIb (higher risk), and Class III (highest risk)[50]. For example, Proteus's wearable sensor, including the IES, has been CE-marked as a Class IIa device in Europe since 2010[4,5]. In addition, medical apps will mostly be classified into Class I, but Class IIa or Class IIb are also possible[51].

In contrast to the US, there is no clear definition of a combination product in the EU[52]. However, article 1(3) of the MDD states that the Medicines Directive shall generally apply in the case of a product that "is placed on the market in such a way that the device and the medicinal product form a single integral product which is intended exclusively for use in the given combination and which is not reusable." Such a 'combination product' is thus classified as a medicinal product and its marketing within an EU member state usually requires the authorization of the competent authorities of that member state[53]. However, in some cases (such as in the case where the medicinal product component is an advanced therapy medicinal product), the marketing authorization is granted by the European Commission through the so-called centralized procedure and is valid throughout Europe[53,54].

A particularly crucial issue that will have to be considered when assessing the safety and effectiveness of IESs is cybersecurity. As a wireless technology, IESs may be targeted by cyber attacks. Not only would this become a costly problem for companies and health-care providers[55], but IESs infected with software viruses, Trojan horses, or worms could also pose a high risk for patients. For example, physicians could give incorrect and unsafe treatment recommendations based on corrupted data. The vulnerability of such technologies was also demonstrated in the WannaCry ransomware cyber attack in May 2017 that affected computers across 150 countries[56]. In particular, in the UK, WannaCry hit the National Health Service (NHS) hard and has resulted in wide-ranging responses by the UK Department of Health and Social Care, NHS England and NHS Improvement such as the production of a 'cyber handbook' that gives guidance in the case of a cyber attack affecting the NHS[57].

An additional problem of cyber attacks is that they pay no heed to national frontiers—data sharing and data breaches will often occur across borders. Thus, it is important that legislators agree upon internationally enforceable, large-scale regulatory cybersecurity frameworks that help to reduce security incidents and prevent IT crime[58]. Setting up such a legislative framework will not be an easy task since it will require the proper balancing of the interests of all private and public stakeholders in their capacity of being IES developers, users, and patients.

Moreover, the new EU General Data Protection Regulation 2016/679 (GDPR)[59] is particularly relevant for IES products and the processing of personal data. The GDPR generally "applies to the processing of personal data", including "data concerning health"[60]. The term personal data means "any information relating to an identified or identifiable natural person ('data subject')"[61]. 'Processing' is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or … use"[62]. 'Data concerning health' is "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status"[63].

In addition to the GDPR's material scope, its territorial scope is also very broad. First, the GDPR does apply in cases where a company is established in the EU and the processing of personal data is carried out in the context of the activities of its relevant establishment, irrespective of whether the processing takes place in or outside of the EU[64,65]. Secondly, the GDPR also applies in cases where a company is not established in the EU (for example, it may be established in the US) and processes the personal data of data subjects who are in the EU and the processing activities are related either to "the offering of goods or services" to these data subjects in the EU or to "the monitoring of their behaviour as far as their behaviour takes place within the Union"[66].

The second processing activity ("monitoring of … behaviour") is especially interesting for IES products. Imagine a US company that has placed an IES product on the US market and a US citizen who uses such a product—with the hope it will improve medication adherence—travels to an EU country during his or her holidays. Does the GDPR apply where the personal data of this US citizen is processed for monitoring his or her medication adherence behaviour that takes place in the EU? According to the European Data Protection Board guidelines, it seems that the GDPR would not apply in such a case since the IES product is exclusively directed at the US market. The GDPR would likely apply when the US company has produced the IES product (also) for the European market and thus aims to target individuals' behaviour within the EU[65]. If the processing of personal data falls within the scope of the GDPR, the US company will usually have to designate in writing a representative in the EU[65,67].

Moreover, legislation similar to the GDPR is evolving in the US: On 28 June 2018, the California Consumer Privacy Act of 2018 (AB-375) was signed into law by former California Governor Jerry Brown. This Act will be operative from 1 January 2020 and, in general, will grant numerous rights to consumers (that is, California residents) concerning personal information relating to them that is held by businesses in the State of California[68].

Conclusions

IESs are a promising technology for improving health outcomes and making health care more effective. The enhanced control over the use and uptake of drugs might even help in the fight against pressing societal problems such as antibiotic resistance. However, IESs also raise ethical and legal challenges. On the ethical side, there are key challenges for IESs relating to patients, physicians, and society more generally. Such issues should be considered at the earliest stages of the development process of such products—the goal is ethics by design—rather than after a product has been designed

and tested. There are also new legal developments in the US and Europe that are relevant for IESs. For example, the US FDA has only recently proposed for public comment a framework for regulating PDURS. In the EU, a new regulatory framework on medical devices (MDR) and in vitro diagnostic medical devices (IVDR) came into force on 25 May 2017. The MDR will generally apply from 26 May 2020 and the IVDR from 26 May 2022. IESs also need to comply with the applicable data privacy laws. As regulators gain more experience with IESs, it is likely (and indeed hoped for) that these pathways will change to facilitate both innovation and high standards of safety and effectiveness as well as data privacy.

For IES products to be broadly accepted by society and markets, it is, in particular, of vital importance to enhance public trust. Hence, companies developing IESs and health-care providers using such products need to gain and maintain patient trust with regard to the management and use of the collected data. Within this trajectory privacy protection, cybersecurity, accountability, transparency, explainability, fairness, and robustness are of pivotal importance.

Received: 16 January 2019; Accepted: 17 July 2019;
Published online: 15 August 2019

References

1. *Digital Health* (FDA, 2018); https://www.fda.gov/medicaldevices/digitalhealth
2. *EHealth: Digital Health and Care* (European Commission, 2018); https://ec.europa.eu/health/ehealth/overview_en
3. *Evaluation of Automatic Class III Designation (De Novo) for Proteus Personal Monitor Including Ingestion Event Marker* (FDA, 2012); https://go.nature.com/2Yt47L6
4. https://www.proteus.com
5. *Qualification Opinion On Ingestible Sensor System For Medication Adherence As Biomarker For Measuring Patient Adherence As Biomarker For Measuring Patient Adherence To Medication In Clinical Trials* EMA/CHMP/SAWP/513571/2015 (European Medicines Agency, 2016).
6. *Proteus Personal Monitor Including Ingestion Event Marker Classification Order* (FDA, 2012); https://go.nature.com/2YiMMQU
7. Council Directive 93/42/EEC, preamble and art. 17; and Directive 98/79/EC, art. 16; and Council Directive 90/385/EEC, art. 12.
8. Otsuka and Proteus announce the first U.S. FDA approval of a digital medicine system: Abilify MyCite (aripiprazole tablets with sensor). *Proteus Digital Health* (14 November 2017); https://go.nature.com/2K1bro3
9. *NDA Approval 207202* (FDA, 2017); https://go.nature.com/2YhpQ4E
10. *Highlights of Prescribing Information: Abilify MyCite (aripiprazole tablets with sensor)* (FDA, 2017); https://go.nature.com/2GsHVXE
11. Proteus Digital Health launches digital oncology medicines to improve patient outcomes. *Proteus Digital Health* (17 January 2019); https://go.nature.com/2XZnHzg
12. Kalantar-Zadeh, K. et al. A human pilot trial of ingestible electronic capsules capable of sensing different gases in the gut. *Nat. Electron.* **1**, 79–87 (2018).
13. https://atmobiosciences.com
14. Mimee, M. et al. An ingestible bacterial-electronic system to monitor gastrointestinal health. *Science* **360**, 915–918 (2018).
15. Subbaraman, R. et al. Digital adherence technologies for the management of tuberculosis therapy: mapping the landscape and research priorities. *BMJ Glob. Health* **3**, e001018 (2018).
16. Muoio, D. Pharmacokinetic study of Proteus' ingestible sensor paves way for clinical trials of HIV prevention drug. *MobiHealthNews* (26 July 2018); https://go.nature.com/2YnOS6s
17. Klugman, C. M., Dunn, L. B., Schwartz, J. & Cohen, I. G. The ethics of smart pills and self-acting devices: autonomy, truth-telling, and trust at the dawn of digital medicine. *Am. J. Bioeth.* **18**, 38–47 (2018).
18. Cohen, I. G. & Pearlman, A. Smart pills can transmit data to your doctors, but what about privacy? *New Scientist* (19 September 2018); https://go.nature.com/2ZbQayu
19. Powell, T. P. The 'smart pill' for schizophrenia and bipolar disorder raises tricky ethical questions. *STAT* (5 December 2017); https://go.nature.com/32PPUrb
20. Zhang, S. Why pharma wants to put sensors in this blockbuster drug. *Wired* (13 November 2017); https://go.nature.com/2K1l4TX
21. Fadus, M. Ethical implications of digital feedback in psychiatric medications. *J. Ethics Mental Health* **10**, 1–7 (2018).
22. *Is The Product A Medical Device?* (FDA, 2018); https://go.nature.com/2JS8PKx
23. FDA clears new robotically-assisted surgical device for adult patients. *FDA* (13 October 2017); https://go.nature.com/2JThZqd.
24. Federal Food, Drug, and Cosmetic Act, s. 201(h).
25. Federal Food, Drug, and Cosmetic Act, s. 513(a)(1)(A)–(C); and Title 21 of the Code of Federal Regulations, ss. 880.2720, 864.7825, 870.3925.
26. Federal Food, Drug, and Cosmetic Act, s. 513(f)(1).
27. *Evaluation of Automatic Class III Designation (De Novo) Summaries* (FDA, 2018); https://go.nature.com/30XSytb
28. Federal Food, Drug, and Cosmetic Act, s. 513(f)(2) and (i).
29. Title 21 of the Code of Federal Regulations, s. 880.6305.
30. 510(k) Clearances K131009, K131524, K133263 and K150494.
31. Title 21 of the Code of Federal Regulations, part 807.
32. Title 21 of the Code of Federal Regulations, s. 801.109.
33. *Frequently Asked Questions About Combination Products* (FDA, 2018); https://go.nature.com/2LFMSjS
34. Robbins, R. A 'digital pill' for cancer patients is rolled out for the first time, in hopes of improving outcomes. *STAT* (17 January 2019); https://go.nature.com/2OrNUCu
35. Molteni, M. Ingestible sensors electronically monitor your guts. *Wired* (24 May 2018); https://go.nature.com/2K0ZCOS
36. *Digital Health Innovation Action Plan* (FDA, 2017); https://go.nature.com/2Ym78Nj
37. FDA. Prescription drug-use-related software; establishment of a public docket; request for comments. [Docket no. FDA-2018-N-3017]. *Fed. Reg.* **83**, 58574–58582 (2018).
38. Council Directive 93/42/EEC of 14 June 1993 concerning medical devices [1993] OJ L169/1.
39. The Treaty on the Functioning of the European Union, art. 288.
40. 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 [2017] OJ L117/1.
41. Medical Device Regulation, art. 123(1).
42. Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices [1990] OJ L189/17.
43. Medical Device Regulation, arts. 122 and 123(2) and (3).
44. Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU [2017] OJ L117/176.
45. In Vitro Diagnostic Medical Devices Regulation, art. 113(1).
46. Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in vitro diagnostic medical devices [1998] OJ L331/1.
47. In Vitro Diagnostic Medical Devices Regulation, arts. 112 and 113(2) and (3).
48. Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use [2001] OJ L311/67.
49. Medical Device Directive, art. 1(2)(a).
50. Medical Device Directive, preamble, art. 9 and annex IX.
51. *Guidance on "Medical Apps"* (German Federal Institute for Drugs and Medical Devices, 2015); https://go.nature.com/2Ym8Nm9
52. Jeary, T. A European perspective and guide to key regulatory considerations for combination products. *Regulatory Rapporteur* **12**, 5–9 (2015).
53. Medicines Directive, art. 6(1).
54. Regulation 726/2004, arts. 3, 13(1), annex I and Regulation (EC) No 1394/2007 of the European Parliament and of the Council of 13 November 2007 on advanced therapy medicinal products and amending Directive 2001/83/EC and Regulation (EC) No 726/2004 [2007] OJ L324/121, art. 2(1)(d).
55. New 'digital' pills pose data protection and cybersecurity challenges for drugs manufacturers and health bodies, says expert. *Out-Law News* (16 November 2017); https://go.nature.com/2GrVuqc
56. Graham, C. NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history. *The Telegraph* (20 May 2017); https://go.nature.com/2y82x2K
57. Smart, W. *Lessons Learned Review Of The Wannacry Ransomware Cyber Attack* (Department of Health and Social Care, 2018); https://go.nature.com/30ZyxSP
58. Mendoza, M. Á. Challenges and implications of cybersecurity legislation. *WeLiveSecurity* (13 March 2017); https://go.nature.com/2JWuhN2
59. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
60. General Data Protection Regulation, arts. 2, 4(15).
61. General Data Protection Regulation, art. 4(1).
62. General Data Protection Regulation, art. 4(2).
63. General Data Protection Regulation, art. 4(15).
64. General Data Protection Regulation, art. 3(1).
65. *Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) — Version for Public Consultation* (European Data Protection Board, 16 November 2018).
66. General Data Protection Regulation, art. 3(2).

67. General Data Protection Regulation, art. 27.
68. California Consumer Privacy Act of 2018 (SB-1121), Legislative Counsel's Digest; Cal. Civ. Code s. 1798.140(g).

Acknowledgements
The research for this contribution was supported by a Novo Nordisk Foundation grant for a scientifically independent Collaborative Research Programme in Biomedical Innovation Law (grant agreement no. NNF17SA027784).

Author contributions
S.G. wrote the first draft and revised the manuscript. T.M. and H.Y. contributed to the manuscript. I.G.C. supervised the work and revised the manuscript.

Competing interests
I.G.C. has served as a consultant for Otsuka Pharmaceutical on their Abilify MyCite product. The company neither funded the preparation of this Perspective nor played a role in its drafting or review.

Additional information
Reprints and permissions information is available at www.nature.com/reprints.

Correspondence should be addressed to S.G.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.