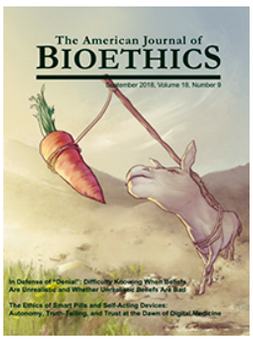

The American Journal of Bioethics

ISSN: 1526-5161 (Print) 1536-0075 (Online) Journal homepage: http://www.tandfonline.com/loi/uajb20

The Ethics of Smart Pills and Self-Acting Devices: Autonomy, Truth-Telling, and Trust at the Dawn of Digital Medicine

Craig M. Klugman, Laura B. Dunn, Jack Schwartz & I. Glenn Cohen

To cite this article: Craig M. Klugman, Laura B. Dunn, Jack Schwartz & I. Glenn Cohen (2018) The Ethics of Smart Pills and Self-Acting Devices: Autonomy, Truth-Telling, and Trust at the Dawn of Digital Medicine, The American Journal of Bioethics, 18:9, 38-47, DOI: 10.1080/15265161.2018.1498933

To link to this article: https://doi.org/10.1080/15265161.2018.1498933

Published online: 20 Sep 2018.

The American Journal of Bioethics, 18(9): 38–47, 2018

ISSN: 1526-5161 print / 1536-0075 online
DOI: 10.1080/15265161.2018.1498933

Target Article

Check for updates

The Ethics of Smart Pills and Self-Acting Devices: Autonomy, Truth-Telling, and Trust at the Dawn of Digital Medicine

Craig M. Klugman, DePaul University
Laura B. Dunn, Stanford University
Jack Schwartz, University of Maryland
I. Glenn Cohen, Harvard Law School

Digital medicine is a medical treatment that combines technology with drug delivery. The promises of this combination are continuous and remote monitoring, better disease management, self-tracking, self-management of diseases, and improved treatment adherence. These devices pose ethical challenges for patients, providers, and the social practice of medicine. For patients, having both informed consent and a user agreement raises questions of understanding for autonomy and informed consent, therapeutic misconception, external influences on decision making, confidentiality and privacy, and device dependability. For providers, digital medicine changes the relationship where trust can be verified, clinicians can be monitored, expectations must be managed, and new liability risks may be assumed. Other ethical questions include direct third-party monitoring of health treatment, affordability, and planning for adverse events in the case of device malfunction. This article seeks to lay out the ethical landscape for the implementation of such devices in patient care.

Keywords: digital medicine; bioethics; nonadherence; professionalism; trust

INTRODUCTION

Digital medicine—combining technological advances in information technology, artificial intelligence, and big data with those of pharmaceutical, biotechnology, and medical device companies—represents a bold new frontier in medical care. Accompanying these technological advances are emerging ethical issues, engendered by the rapid pace of technology and the challenges of managing vast amounts of patients' medical, behavioral, and personal information. This article briefly describes digital medicine, highlights several ways in which digital medicine may lead to improved patient outcomes, and uses an illustrative case of digital medicine targeting the problem of medication adherence to identify evolving ethical issues in this area.

DIGITAL MEDICINE: WHAT AND WHY

"Digital medicine is the transformation of health care that is coming about as computer technology is used in the creation and application of medical knowledge" (Shafer and Kigin 2002, 200). These technologies may provide a wide array of novel approaches in health care, including continuous and remote monitoring, digital phenotyping, remote disease management, and self-reporting, self-tracking, and self-management (Elenko et al. 2015). The Food and Drug Administration (FDA) folds digital medicine into the category of *digital health,* which is any "mobile health, health information technology, wearable devices, telehealth, telemedicine, and personalized medicine" (FDA 2017). Digital medicine devices are intimate in that they either touch the surface

Address correspondence to Craig M. Klugman, Department of Health Sciences, DePaul University, 1110 W. Belden Avenue, Suite 411, Chicago, IL 60614, USA. E-mail: cklugman@depaul.edu

of a person's body, or are ingested, inserted, or implanted into the body. They also record information that can be stored, tracked, and shared.

While most efforts in the broader digital health category have focused on data collection, management, and analysis, emerging forms of digital medicine seek to combine device technology with medication. These novel products aim to enhance health by providing improved ways to measure, monitor, and administer treatment. For example, the t:slim X2 insulin pump with Dexcom G6 Continuous Glucose Monitor (CGM) system for diabetes care provides 24-hour recording of a patient's glucose levels. These readings can be sent automatically and electronically to up to five other people. In addition, when the system detects a rise in glucose, it automatically releases the proper amount of insulin to the patient's bloodstream (Tandem 2018).

As described by some authors, the goals of digital medicine include: the "generation and application of medical knowledge that will make health care safer and more effective by enhancing our ability to diagnose and treat disease" (Shafer and Kigin 2002, 200). These authors opine that such efforts should make medicine more precise, effective, innovative, widely distributed, and egalitarian (Shafer and Kigin 2002). However, the fruits of these digital medicine labors have yet to be harvested, so these assertions will need to be rigorously tested as these technologies are rolled out.

TREATMENT ADHERENCE AND DIGITAL MEDICINE

One putative role for digital medicine technologies may be to develop new approaches to improving treatment adherence (Fleurant 2008). Adherence is the degree to which a patient follows medical advice, most commonly with regard to taking medications. Nonadherence to prescribed medications is a significant problem across all medical fields, and limits providers' abilities to fulfill their ethical obligation of working to improve patients' health and well-being. Up to 25–50% of patients do not take their treatments as prescribed, threatening their health and well-being (DiMatteo 2004). Among patients with some disorders (e.g., schizophrenia, diabetes, asthma), nonadherence is the largest driver of relapse and hospitalization (Ascher-Svanum et al. 2010; Iuga and McGuire 2014; Sun et al. 2007). In addition to the financial costs of nonadherence, patients who do not adhere to their medications face other potentially serious consequences, including higher rates of complications and death (Ho et al. 2006). The cost of additional treatments and hospitalizations from nonadherence is estimated to be in the billions of dollars annually (Iuga and McGuire 2014).

Reliably identifying medication nonadherence is both clinically important and challenging. When patients do not respond to a medication, it can be difficult to determine whether the lack of response is due to nonadherence or whether the medication itself is not effective. Traditionally, clinicians had to rely on patients' self-reporting of adherence to medications. Studies show that self-reporting is unreliable: Patients may have inaccurate memories of taking their medications or may be embarrassed to admit failure to comply or inability to access (lack of finances, not understanding instructions, memory problems) medications (Stirratt et al. 2015). Scholars have pointed to the need for a more accurate measure of whether and when patients take their medications (Garfield et al. 2011). Although some technological advances (e.g., an electronic medication container lid) can provide information related to medication adherence, they do not provide direct evidence of medication ingestion. Digital medicine may do so.

Products that incorporate adherence monitoring are already on the market and others are awaiting FDA approval. For example, Rush University is using a compound pharmacy to combine existing medications with an ingestible sensor, developed by Proteus Digital Health, that emits a weak signal when the medication is ingested (the stomach acids act as a battery for a few moments before those same acids dissolve the sensor). This weak signal is relayed via a patch worn on the abdomen that links with a smartphone app and records that the medication was taken. The app can share information with clinicians and others in hopes of helping patients to take their medications as prescribed (Holly 2017). Another example is Otsuka Pharmaceuticals' recent FDA approval of a combination of the Proteus sensor with the drug Abilify (i.e., aripiprazole, which is currently FDA approved for a range of indications in the treatment of serious mental illnesses). This combination, called MyCite, uses an app to record patients' ingestion of their medication. The app can also track, if the patient wishes, additional information such as self-reported mood and sleep ratings (Otsuka Pharmaceuticals 2017). What these devices have in common is automated collection of patient information (glucose levels, medication ingestion), the ability to share that information with designated others, and the link to medication (ingesting a pill, signaling a dose of insulin).

ETHICAL ISSUES IN DIGITAL MEDICINE

Prior ethics-related literature has focused primarily on challenges raised broadly by digital health rather than on those specific to digital medicine (Rippen and Risk 2000). This literature tends to address concerns and risks related to electronic information sharing only. Given that the technologies for combining electronic monitoring and medication only developed more recently (i.e., Proteus received FDA approval for its ingestible sensor in 2012, and Dexcom for its continuous glucose monitoring device in 2015), there remains a need to examine the ethical landscape of digital medicine as these new drug-device technologies enter the market and become more widely used. This article seeks to map that landscape.

For this discussion, we divide the ethical issues into those that predominantly affect the patient, the provider, and society. We fully recognize that some ethical issues may implicate more than one category, and we do not present this categorization as sacrosanct but instead as a helpful heuristic.

Patient Issues

Digital medicine creates a variety of unique ethical issues for patients who are treated and monitored with these devices. These drug-device technologies hold implications for autonomy and informed consent, device-related "therapeutic misconception," data management, undue influence, privacy and confidentiality, and dependability.

Autonomy and Informed Consent

Informed consent is the patient's exercise of autonomy by voluntarily agreeing (or disagreeing) to participate in a test, procedure, or research study. In many clinical situations, consent for noninvasive, generally understood, testing is presumed from the patient's cooperation (e.g., the clinician says, "I'm going to take your blood pressure now" and performs that action unless the patient refuses). For invasive procedures, consent is usually more explicit and made in writing. When writing is involved, such documents are crafted by medical staff, sometimes in consultation with legal counsel, and present a patient with a description of the process, risks, benefits, and alternatives.

Digital medicine, by contrast, provides a new challenge: The use of a digital medicine product may be governed by a user agreement in addition to the traditional informed consent process. For example, when the patient registers his or her digital medicine app or device, he or she will be prompted to indicate agreement. User agreements tend to be long documents (e.g., Apple's iTunes agreement is 56-pages long (Pidaparty 2011)), written by lawyers, are typically contracts of adhesion and thus not negotiable (i.e., if you do not agree, then you do not get to use the product), can be changed at any time and without notice, and spell out the terms under which the software and hardware can be used: appropriate ways to use the technology, the limits of use, and protections for the company.

Issues of comprehension—a key element of informed consent—may come into stark relief in the context of digital medicine and the user agreement. In an informed consent process, a provider speaks to the patient and this exchange culminates in the patient's permission (or refusal) for treatment or diagnosis. A user agreement, however is framed explicitly as a contract that one agrees to without engaging in a face-to-face conversation. Informed consent is primarily for the benefit of the patient, but user agreements are primarily designed to benefit the companies. A patient using digital medicine will be part of two overlapping but distinct processes: consent for what the clinician prescribes, and mere acquiescence to the terms dictated by the company. This may cause confusion and may be a threat to a patient's perception of or actual exercise of autonomy: Not agreeing means not receiving this particular device, and thus the patient may feel that she or he has no choice.

Furthermore, when a patient agrees to a digital medicine user agreement, they may not understand that they are also agreeing to maintenance and updates to the device. Digital medicine devices, unlike medication alone, may require ongoing maintenance such as battery changes, sensor replacements, and software updates. Moreover, the technology underlying digital medicine may experience failures for various reasons. Companies will need to keep track of device data in order to provide this necessary servicing, as well as to continually improve the machine and perform quality control. These issues are similar to those faced by patients with implantable technologies (pacemaker, left ventricular assist device [LVAD], defibrillator) with the exception that an app can be uninstalled and a patch taken off by the patient, but an implantable device requires surgery to remove.

Technology advances at a far more rapid rate than pharmaceutical development. Access to data is essential for continuing development of these technologies (Cohen et al. 2014). These updates are built on analyzing the data of previous iterations. User agreements might be written in such a way that companies require access to patient data for these necessary purposes. This raises the ethical question of whether patients should have the option of not allowing their data to be used for medical research or product development.

Maximally empowering patient autonomy would mean giving patients an absolute right to provide or refuse consent for their data to be used in research. However, some scholars have suggested that, at least in the setting of research aimed at expanded knowledge about potentially lifesaving or life-changing treatments, citizens owe an obligation to contribute to the public good by volunteering for research, much as they are obliged to contribute to other public goods by paying taxes (McCormick 1974; Schaefer et al. 2009). Although private-sector product development is not directly comparable, digital medicine combines a prospect of benefit to large groups of patients with an exceptional need for quickly identified and implemented product refinement. Some might argue, therefore, that patients who voluntarily agree to use digital medicine are also agreeing, in effect, to contribute to the well-being of the next cohort of users through an obligation to share their deidentified data.

That is, in digital medicine, the need for constant improvement and maintenance suggests that at least patients deidenitified[1] data should always be part of

1. Deidentification is a moving target and better conceived of as a continuum, since only useless data are truly completely deidentified. Under the updated Common Rule for human subjects research, a new provision states that standards of deidentification will be updated every 4 years.

digital medicine research. However, even patient's identifiable data may be necessary for quality improvement of these devices: For example, if a device fails, knowing that the patient was swimming with his or her smartphone is important. In all cases, digital medicine user agreements should be plainspoken about future data use. Patients should be informed of whether the data to be stored will be identifiable, deidentified, or coded (maintained with a code easily traceable back to an individual), and how the company plans to use the information. Any changes to the user agreement affecting data use should be highlighted, and an opportunity to re-consent or withdraw consent should be offered. To be sure, this may mean that when terms change and patients do not like the new terms, they may need to discontinue use of the product. Different arrangements may be necessary for products that are implanted or otherwise difficult to discontinue use, but those products are beyond the scope of this discussion.

Device-Related "Therapeutic Misconception"

A patient is prescribed a continuous glucose monitoring device. The machine collects information and sends alerts to the patient and to any other designated individuals. Alone, the device does not administer medical treatment, although it can be combined with an insulin pump. One challenge to patient autonomy in this situation is the potential for a form of device-related "therapeutic misconception" (Appelbaum et al. 1982; Henderson et al. 2007). Therapeutic misconception, originally described in the clinical research setting, refers to a research participant failing to appreciate crucial distinctions between the nature, purpose, and potential benefits of research versus those of individualized clinical care (Appelbaum et al. 2004; Lidz et al. 2015). In the context of digital medicine, there is a risk that patients using devices may not understand that the device itself does not provide treatment, or patients may not be able to distinguish between the monitoring portion and the active drug. Given the complexity of evolving drug-device digital medicine technologies, the risk of such misconceptions (or others we have not identified) may be elevated. Gathering empirical data on the frequency and characteristics of such misconceptions therefore would be useful as digital medicine emerges.

In the case of medication adherence monitoring, there may also be important misconceptions about how closely the clinician (or other individuals) will be monitoring the patient through the digital medicine product. Digital medicine may enable but not require the clinician to monitor the patient's data that is collected by the device, and will certainly not require clinicians to check their incoming data a requisite number of times in a fixed period. Patients may believe and indeed opt for digital medicine over older formulations of the same product precisely to obtain closer monitoring. However, this expectation may be unfounded, or may be an overestimation of the level of scrutiny the clinician will be able or willing to give to the patient's data. Studies of remote monitoring of cardiac patients have shown that patients feel comfortable using smartphones for monitoring but physicians are more reluctant—expressing concerns about unreimbursed time, liability, and whether the data are actually useful (Achituv and Haiman 2016; Seto et al. 2010). Therefore, beyond any questions of informed consent, it is essential that patients and clinicians reach a meeting of the minds as to whether patients' expectation of monitoring meets clinician reality.

A different approach to this problem is to consider issues of choice architecture in digital medicine product design. The concept of choice architecture, which was popularized by Richard Thaler and Cass Sunstein in their work on nudges, aims to design interventions to influence behavior without infringing on freedom of choice (Thaler and Sunstein 2008). Whenever a system provides information to a clinician, the setting of "defaults" represents a powerful and often overlooked way of shaping behavior (Cohen et al. 2014). If alert settings, as with many defaults, remain "sticky"—clinicians are unlikely to change the settings—then by setting default rules for providing alerts to clinicians, a digital medicine product may succeed in shaping how frequently clinicians attend to the information the system provides. However, clinicians are rightly wary of alert fatigue, which is correlated with a high frequency of alerts and may contribute to provider burnout (Ancker et al. 2017).

Data Management

In digital medicine, patients have new responsibilities when it comes to their data. Consider that the device is recording data both automatically—blood sugar levels, body temperature, ingestion of pill—and manually—patient enters mood, hours of sleep, and energy level. First, patients must decide who has access to this data. The patient may give permission for other individuals to access the data, whether through an online portal or even through push notifications. Thus, the data may be shared with the clinician, family members, friends, the pharmaceutical manufacturer, the hardware and software companies, insurers, and even a peer network.

Whether a patient retains a legal right to control these data may depend on a host of factors, such as whether the data have been deidentified or not, what jurisdiction the data are collected in, whether the data are collected as part of human subjects research, and so on. What is needed is the development of best practices regarding patient data digital medicine products. If one's goal is widespread adoption of digital medicine, maintaining the trust of patients is essential, and hewing only to the least demanding legal standard is unlikely to achieve an ethical practice of digital medicine.

At a bare minimum, respect for persons requires clear and comprehensible information available to patients on what is being done with the patient data and who, if anyone, has the right to view those data. The patient should be able to grant or rescind access to individuals or cease using the device to terminate sending data to the manufacturer. The thornier issue is whether patients should have the further right to withdraw data they have already contributed. Doing so would maximally respect patient rights of privacy and data control, but poses significant logistical challenges for companies seeking to implement these solutions. It might also jeopardize their ability to improve the digital medicine products. One possible compromise would be to provide the patient a right to withdraw identified data, but not aggregated deidentified data, on the theory that the individual patient interest in such data is highly diminished.

In truth, the right answer probably depends on a series of more context-specific issues, such as the risk/difficulty in re-identification, how sensitive the data in question are, how important data retention is, not just to the commercial interests of the company making the product but to the patients who benefit from improvements, and so on. There are no pat answers, but we think these considerations are the ones that can appropriately shape the debate as to ethical policy for such products.

External Influences

Consent may be further compromised by the beliefs and requirements of another party. In theory, could a clinician state that she will only work with the patient if he agrees to the digital medicine solution? Currently, clinicians sometimes require patients to agree to certain behavioral conditions in order to continue treating them (e.g., coming to appointments, undergoing urine drug testing). There may be disagreement among clinicians regarding whether such conditions represent a kind of "external influence"—that is, pressuring the patient to do something he or she otherwise would not. Other examples of potential influences on patient's use of (or clinicians' prescribing behavior) include an insurance company's expressing preference for the digital version of a medication if it has data showing that using such pills reduce their costs, or, conversely, an insurer refusing to cover digital medicine because of a lack of data on reducing costs.

On the other hand, what if a patient wants the digital solution because she or he feels this will really help and the clinician does not agree with the use of such devices or with the specifics of the user agreement? Without the clinician's prescription, the patient cannot get the solution. After all, clinicians are the gatekeepers to prescription medications and devices. Torous and Roberts wrote that there is currently no evidence these digital devices improve adherence or patient outcomes (Torous and Roberts 2017a, 2017b). Of course, the lack of data may be a result of few solutions being on the market. Perhaps a clinician who refuses to write the prescription should refer the patient to a colleague who would? Arguably, this is similar to a patient who shops for another clinician who will prescribe the desired specific medication, such as antibiotics for a viral infection or opioids unrelated to organic pain. The physician's bias, whether based on evidence or on morality, can be a factor in patient access.

Initially, digital medicine devices are likely to be optional for patients if they consent and agree to the monitoring, sharing of information, and extra costs, and if their insurer agrees to pay. However, if these devices demonstrate that they do improve health outcomes and reduce long-term costs, then this option could become a requirement. Insurance companies may prefer these devices and encourage patients to use them through financial incentives. The option of information sharing could easily slip into a requirement. The preferred treatment may require relinquishing some privacy.

For example, if Proteus's sensor makes its way into other types of pills (contraception, Alzheimer's medication, direct observed therapy for tuberculosis), then these might become required. A person on directly observed therapy for treating tuberculosis might find more freedom with an automated solution that does not require daily nurse visits to ensure medication adherence. To play this forward into more disturbing territory, could a court mandate that a person on probation submit to medication adherence monitoring? Could a psychiatrist threaten involuntary hospitalization unless a patient agrees to adherence monitoring technologies? The slippery slope risk is that monitoring our internal health and our medication use could be removed from our personal locus of control to an external one. These devices raise questions that, if not properly addressed, could degrade autonomy.

Preserving the Confidentiality of Private Data

One of the features of these devices is the ability to share information with others: often one's clinician, family, or friends. However, in the practice of medicine, patients have an expectation of privacy grounded in law, professionalism, and ethics. Patients give up their private information to a health care provider who will use the information to diagnose and treat while maintaining confidentiality—protecting the patient's secrets. Family and friends of adult patients are typically not thought of as having such fiduciary duties, or at least not in a legally enforceable sense. Should families and friends who undertake to receive adherence monitoring or other digital medicine data be required to also undertake duties of confidentiality comparable to those that characterize the clinician–patient relationship? If so, then are those duties best thought of as moral norms or should they be encoded in law?

Other parties could also expect access to the data, such as an insurance company, programmers and managers at the cloud storage service, a pharmaceutical manufacturer, or a device manufacturer. The use of such data in the judicial system may raise particularly thorny issues. In one reported case, police sought a search warrant to access pacemaker data of a patient they suspected of arson (Telltale heart: Pacemaker data leads to arson, fraud charges 2017). As digital medicine use expands, though, such cases are likely to become more frequent and varied. Imagine that at the sentencing phase for a patient who has committed a violent act during a psychotic break, prosecutors seek adherence monitoring data from digital medicine to show that the patient is likely to be a danger to society because he does not take his antipsychotic medication as prescribed.

Dependability

Even if the system is perfectly safe and secure, there is also the risk that the technology could fail (Giota and Kleftaras 2014). A patient may become dependent on the system, but these devices sometimes stop working—batteries wear down, software becomes corrupted, even networks fail. Across all technologies, user error is a frequent issue, and likely to be more so with complicated devices that require sensor patches to be changed, batteries to be charged, and software to be used correctly. A patient might not realize that her glucose is no longer being monitored or that a pill fails to register, assuming that the technology is working. Digital medicine manufacturers have an obligation to thoroughly test the dependability of their product, assess risks in the overall system for data authentication, transmission, and storage, and assess the ease of use through rigorous human factors testing.

Regulators like the FDA that approve these products will also need to develop expertise in evaluating these issues. If these devices fail to work as advertised, at the least patients may lose trust in digital medicine and at the most, may risk harms to their health.

Provider Issues

Digital medicine creates a variety of unique ethical issues for the clinician who will be treating and monitoring patients with these devices. These drugs and devices hold implications for transforming the clinician–patient relationship, patient trust, clinician monitoring, managing expectations, and liability risks.

Transforming the Clinician–Patient Relationship

With traditional pharmaceuticals, the clinician prescribes the medication, the patient has the prescription filled at a pharmacy, the patient takes the drug (or does not), and at some later date, the patient and clinician talk to see whether the drug has worked. Digital medicine is closer to telemetry, where the patient is consistently and closely monitored. For example, the t:slim X2 insulin pump with Dexcom G6 Continuous Glucose Monitor (CGM) system gives the clinician near-real-time access to the patient's blood sugar levels and administration of insulin. This level of monitoring may be new to many areas of medicine, such as outpatient psychiatry. The adherence-monitoring version of the same drug or drug delivery device may change the clinician–patient relationship, a change that can have benefits and concerns.

Psychiatrists Torous and Roberts believe that "technologies should serve to enhance the psychiatrist–patient relationship, rather than replace it" (Torous and Roberts 2017a). Closer monitoring could theoretically lead to better patient outcomes and lower costs. A clinician may have to spend less time with each patient because more data are available before an office meeting. Perhaps the patient's follow-up appointments could be spaced further apart, as the clinician will know the patient's self-reported mood and automatically logged adherence on a regular basis. This could reduce cost for the patient and the insurer, as well as allowing the clinician to treat more patients. However, the change also means that some aspects of practice will be transformed.

Patient Trust

With digital medicine, the clinician can log into a portal and verify if a patient has taken the medication or acted on an aberrant reading. If the device permits patients to add extra information (like mood, diet, sleep), then there may be more data to see whether the medication is having an effect. The clinician will know whether ineffectiveness is due to the medication or nonadherence because she or he can see how often and when the drug was taken. The backbone of the clinician–patient relationship has always been trust—trust that the clinician aims to help the patient and preserve confidentiality.

The clinician, in turn, trusts that the patient wants to get better and will follow prescribed instructions. Sometimes, however, the clinician develops a suspicion of nonadherence, despite the patient's insistence to the contrary. This uncertain state—the clinician skeptical but unsure, the patient insistent but perhaps ashamed—can erode trust. With digital medicine, whether the patient has carried out instructions is independently verified; the clinician does not have to depend on the patient's word. It could be argued, on the one hand, that eliminating uncertainty about the patient's actual behavior could bolster trust by redirecting discussion away from the patient's veracity toward the reasons for nonadherence. On the other hand, not all patients will see it this way. Some may prefer to be able to deceive their clinicians, and this technology threatens their ability to do so. Whatever one thinks about whether patients have a

"right to deceive" their physicians in this way, when a treatment has a digital medicine and analog version, patients who want to retain this "right" can choose not to pursue the digital medicine formulation.

Monitoring the Clinician

But there is also a different kind of trust relationship at stake—the relationship of industry and clinicians. Insurers may use digital medicine devices to monitor and evaluate clinicians. Medical device manufacturers and pharmaceutical companies—which have always had access to patient prescribing patterns through the American Medical Association (AMA)—will now have access to when and how their products are used, not just whether they were prescribed. Data portals will require usernames and passwords, which will track when a clinician logs on, how much time is spent looking at information, and perhaps whether any adjustments were made to the digital medicine device (e.g., the app's settings). Some of this information may be helpful for designing user-friendly and easier-to-use software, but it could also be designed to determine whether clinicians do keep closer tabs on their patients. If a company wants to demonstrate that its digital medicine technology improves health outcomes and reduces costs, it may require (in the user agreement) access to corroborating medical records. Clinicians may find themselves subject to greater oversight monitoring and further erosion of professional autonomy at the hands of insurers and manufacturers. Whether physicians would be willing to give up more of their professional autonomy has not been studied.

Drawing the line between appropriate and inappropriate monitoring of providers will present thorny issues. It does not seem prima facie wrong for an insurer to seek to know whether the clinician is actually monitoring adherence before it agrees to reimburse for a more expensive digital medicine version of a product. But what about an insurer that uses this to develop clinician-specific profiles that go far beyond the purpose of the product and help it to evaluate whether to keep a particular clinician in network? Clinicians will be unlikely to adopt digital medicine products, even those that promise significant benefits for their patients and society, if they think that by doing so they are making themselves vulnerable to robust insurer monitoring.

Managing Expectations

As discussed in the section on patient autonomy, now that clinicians will have access to patient behavior, the patient may expect the clinician to be checking. If a clinician has several hundred patients, a daily or weekly check into everyone's portal, and following up, could consume a greater amount of time. In this regard, it is worth highlighting how payment models may have an important role to play in promoting better digital medicine usage. If the time clinicians spend reviewing data from digital medicine products, including adherence, is not compensable time, many fewer clinicians will spend the time to monitor patient data in the way these products are designed to enable.

These devices may actually increase the time providers spend managing patient adherence. For example, patients may skip appointments, thinking that if there is a problem then their health care provider will contact them: GCM sends an alert if glucose levels change (Dexom 2018). After all, the data are flowing at a constant rate: Pills are taken at roughly the same time every day and continuous glucose monitoring sends data to storage (and the information portal) every 5 minutes (Dexom 2018). Digital medicine and health will change the provider–patient relationship (Anderson and Goodman 2002).

Liability Risks

Even if user agreements and consent forms spell out that the clinician is under no obligation to check the data, the patient may expect this. The insurer may also expect it—after all, why pay more for digital medicine if the tool goes unused? For some of these technologies there may be an expectation that the information will be incorporated into clinical records. The use of these technologies may also trigger the need to comply with the federal privacy rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Could a clinician who does not keep tabs on the data be liable for failure to do so if there is a bad outcome? A diabetic patient who goes into ketoacidosis that could have been avoided if the clinician's office had just checked might face a lawsuit. Or, as discussed in the preceding section, perhaps a clinician changed a default setting (such as send notification every 24 hours to once a week). When, after an adverse event, a patient sues a provider for medical malpractice, a key question is whether the provider's behavior comported with the relevant standard of care. The sources of information on that standard of care are multifarious—expert testimony, practice guidelines, and so on—but in setting certain defaults for alerts (already discussed) and other actions, digital medicine products may contribute to standards of care for these products. Cohen et al. ask whether courts will afford clinicians leeway when determining how best to use such data (Cohen et al. 2014).

Societal Issues

Some of the ethical issues raised by these technologies fall outside of the provider–patient/family relationship: (1) With the greater connectivity and information these devices make available, third parties may have an interest in access; (2) given the cost of such technologies, there may be issues of affordability; and (3) trust

requires transparency to the public for reporting adverse events.

Insurers

Digital medicine is a more expensive alternative to traditional therapy. Continuous glucose monitoring may be more effective for some patients to control their glucose and A1C levels, but that could be managed through finger sticks even if those are less convenient, more painful, and more burdensome (Juvenile Diabetes Research Foundation Continuous Glucose Monitoring Study et al. 2009). A GCM unit costs around $1200 plus $500 once a year for a battery, and sensors of $35 to $100 that must be changed at least once a week. Traditional testing strips and supplies cost less than $800 a year (Yeaw et al. 2012). Otsuka's digital medicine produce is priced at nearly double the cost of non-digital Abilify along (Robbins 2018). Insurance companies are likely to want proof that there is benefit to the additional costs. The goal of better adherence is preventing more expensive care later. Thus, insurers may demand access to patient information showing that patients are indeed using the devices. Or the insurer may require clinicians to log into the tracking portal a certain number of times per week to track patient use. In an ideal world, patients' decisions to share this kind of information would be completely free. However, some might argue that an insurer may have a legitimate contrapuntal interest: not to waste resources. Such a claim becomes particularly strong when a payer is a public one such as Medicaid or Medicare and the resources used to support digital medicine are in some sense communal.

Equitable Access

Both the Dexcom and the Otsuka products require the use of a smartphone to send information from the sensor to the cloud server and portals. According to the Pew Research Forum, 77% of U.S. adults have a smartphone (Smith 2017). However, smartphone ownership is correlated with income level: While 93% of adults who make more than $75,000 per year own these devices, only 64% of those who make less than $30,000 per year do (Pew Research Center 2017). Thus, if having a smartphone is a requirement of using digital medicine, then the solution is less available to those of lower socioeconomic status. It would be ethically preferable, under principles of social justice, to ensure that patient access to these technologies is not dependent on socioeconomic status. It is thus incumbent on digital medicine companies to take steps to improve access to these solutions to patients on the other end of the digital divide. This might include establishing technology loaner programs, designing the products to work with cheaper smartphone models, or subsidizing access for poor patients, though all of these efforts would need to be vetted through the complex web of anti-kickback laws (Office of Inspector General 2002, 2003, 2016).

Transparency

As a result of the potential technological problems with these devices, companies will need to be transparent with clinicians and patients about all aspects of digital medicine. Patients and providers have always had to trust pharmaceutical companies and FDA testing that medications are safe and effective. Digital medicine will also require trust, but because the device changes are frequent (software updates, security patches, monitoring) and the potential for failure is different (mechanical difficulties, hacking), a greater level of trust is required. One way to ensure this is for manufacturers to adopt transparency policies and include them in the user agreement (Torous and Roberts 2017b). If devices are hacked or problems are discovered, it's important that clinicians and patients receive timely information. Response must be immediate to notify end users about problems and correct them. GCM issues could suggest that patients go back to finger pricks for a while. For pill logging, patients should know whether the monitor is malfunctioning or corrupted so they can go to a paper log or other alternative reporting method.

THE FUTURE

With Congress funding the 21st Century Cures Act, the FDA rolling out regulations and review structures for such devices, and $8 billion invested in drug companies, device manufacturers, and the National Institutes of Health, the future of treating disease is digital (Cortez et al. 2017; FDANews 2017; Greenwood 2017).

Bioethics has only begun to scratch the surface of the issues this new technology raises.

Digital companies and the bioethics community should actively engage with the issues described in the preceding section. Anticipating, planning for, and iteratively addressing the array of ethical issues throughout products' life cycles will enhance patient, professional, and public trust in these emerging technologies. Importantly, involving not only ethicists but also patient groups, practicing clinicians, and payors in these conversations will also further this goal. Finally, the ethical issues need to be examined on a continuing basis—rather than at one point in time—as the technology is evolving so rapidly. The bioethical debates may take on different dimensions when we consider a future where individuals may interact with many different devices as compared to a single device. We do not know, for instance, whether at some point the total weight of a digital medicine panopticon may become too great, even if each individual device was acceptable on its own.

FUNDING

Cohen's work was supported by the Collaborative Research Program for Biomedical Innovation Law, which is a scientifically independent collaborative research program supported by Novo Nordisk Foundation (grant NNF17SA0027784).

DISCLOSURE STATEMENT

All four authors served as consultants for Otsuka Pharmaceuticals, advising on the use of digital medicine. The company neither funded the preparation of this article nor played a role in its drafting or review. ■

REFERENCES

Achituv, D. B., and L. Haiman. 2016. Physician's attitudes toward the use of IoT medical devices as part of their practice. *Online Journal of Applied Knowledge Management* 4(2): 2016.

Ancker, J. S., A. Edwards, S. Nosal, D. Hauser, E. Mauer, R. Kaushal, and With The H. I. 2017. Effects of workload, work complexity, and repeated alerts on alert fatigue in a clinical decision support system. *BMC Medical Informatics and Decision Making* 17(1): 36. doi:10.1186/s12911-017-0430-8

Anderson, J. G., and K. W. Goodman. 2002. *Ethics and Information Technology: A Case-Based Approach to a Health Care System in Transition*. New York: Springer.

Appelbaum, P., C. Lidz, and T. Grisso. 2004. Therapeutic misconception in clinical research: Frequency and risk factors. *IRB* 26(2): 1–8.

Appelbaum, P. S., L. H. Roth, and C. Lidz. 1982. The therapeutic misconception: informed consent in psychiatric research. *International Journal of Law Psychiatry* 5(3-4): 319–329.

Ascher-Svanum, H., B. Zhu, D. E. Faries, et al. 2010. The cost of relapse and the predictors of relapse in the treatment of schizophrenia. *BMC Psychiatry* 10(1): 2. doi:10.1186/1471-244X-10-2

Cohen, I. G., R. Amarasingham, A. Shah, B. Xie, and B. Lo. 2014. The legal and ethical concerns that arise from using complex predictive analytics in health care. *Health Aff (Millwood)* 33(7): 1139–47. doi:10.1377/hlthaff.2014.0048

Cortez, N. G., N. Terry, and I. G. Cohen. 2017. Questions about the FDA's new framework for digital health. *Health Affairs Blog* Available at: http://healthaffairs.org/blog/2017/08/16questions-about-the-fdas-new-framework-for-digital-health/

Dexom. 2018. The new Dexcom G6 CGM is here. Available at: https://www.dexcom.com/g6-cgm-system

DiMatteo, M. R. 2004. Variations in patients' adherence to medical recommendations: A quantitative review of 50 years of research. *Medical Care* 42(3): 200–209.

Elenko, E., L. Underwood, and D. Zohar. 2015. Defining digital medicine. *Nature Biotechnology* 33(5): 456–461. doi:10.1038/nbt.3222

FDA. 2017. Digital Health. Available at: https://www.fda.gov/medicaldevices/digitalhealth/

FDANews. 2017. Otsuka and Proteus Digital Health Resubmit Application to FDA for Digital Medicine Device. Available at: http://www.fdanews.com/articles/181895-otsuka-and-proteus-digital-health-resubmit-application-to-fda-for-digital-medicine-device

Fleurant, M. 2008. High-tech, simple solutions for improving patient care management. *Biotechnology Healthcare* 5(3): 35–38.

Garfield, S., S. Clifford, L. Eliasson, N. Barber, and A. Willson. 2011. Suitability of measures of self-reported medication adherence for routine clinical use: A systematic review. *BMC Medical Research Methodology* 11(1): 149. doi:10.1186/1471-2288-11-149

Giota, K. G., and G. Kleftaras. 2014. Mental health apps: Innovations, risks and ethical considerations. *E-Health Telecommunication Systems and Networks* 3:13–23. doi:10.4236

Greenwood, L. 2017. Money is rapidly flowing into the digital health spac. *MassBio News* Available at: https://www.massbio.org/news/blog/money-is-rapidly-flowing-into-the-digital-health-space-134772

Henderson, G. E., L. R. Churchill, A. M. Davis, et al. 2007. Clinical trials and medical care: Defining the therapeutic misconception. *PLoS Medicine* 4(11): e324. doi:10.1371/journal.pmed.0040324

Ho, P. M., J. S. Rumsfeld, F. A. Masoudi, et al. 2006. Effect of medication nonadherence on hospitalization and mortality among patients with diabetes mellitus. *Archives of Internal Medicine* 166(17): 1836–1841. doi:10.1001/archinte.166.17.1836

Holly, R. 2017. This 'smart pill' can help rush patients remember their meds. *Chicago Tribune*, 2017 (June 27). Available at: http://www.chicagotribune.com/bluesky/originals/ct-bsi-proteus-smart-pill-20170616-story.html

Iuga, A. O., and M. J. McGuire. 2014. Adherence and health care costs. *Risk Management and Healthcare Policy* 7:35–44. doi:10.2147/RMHP.S19801

Juvenile Diabetes Research Foundation Continuous Glucose Monitoring Study, Bode, G., B. Beck, R. W. Xing, et al. 2009. Sustained benefit of continuous glucose monitoring on A1C, glucose profiles, and hypoglycemia in adults with type 1 diabetes. *Diabetes Care* 32(11): 2047–2049. doi:10.2337/dc09-0846

Lidz, C. W., K. Albert, P. Appelbaum, L. B. Dunn, E. Overton, and E. Pivovarova. 2015. Why is therapeutic misconception so prevalent? *Cambridge Quarterly of Healthcare Ethics* 24(02): 231–241. doi:10.1017/S096318011400053X

McCormick, R. A. 1974. Proxy consent in the experimentation situation. *Perspectives in Biology and Medicine* 18(1): 2–20.

Office of Inspector General. 2002. *Offering gifts and other indecements to beneficiaries*. Washington DC: DHHS. Available at: https://oig.hhs.gov/fraud/docs/alertsandbulletins/sab giftsandinducements.pdf.

Office of Inspector General. 2003. Compliance Program Guidance for Pharmaceutical Manufacturers. Available at: https://oig.hhs.gov/fraud/docs/complianceguidance/042803pharmacymfgnonfr.pdf

Office of Inspector General. 2016. Medicare and state health care programs: Fraud and abuse; revisions to the safe harbors under the anti-Kickback Statute and civil monetary penalty rules regarding beneficiary inducements. *Federal Register* 81(235): 88368–88409. Available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-07/pdf/2016-28297.pdf

Otsuka Pharmaceuticals. 2017. Ostuka and Proteus Digital Health Resubmit Application to FDA for First Digital Medicine. Available at: https://www.otsuka-us.com/discover/articles-1033

Pew Research Center. 2017. Mobile Fact Sheet. Available at: http://www.pewinternet.org/fact-sheet/mobile/

Pidaparty, U. 2011. What you should know about iTunes' 56-page legal terms. *CNN* Available at: http://www.cnn.com/2011/TECH/web/05/06/itunes.terms/index.html

Rippen, H., and A. Risk. 2000. e-health code of ethics (may 24). *Journal of Medical Internet Research* 2(2): e9. doi:10.2196/jmir.2.2.e9

Robbins, R. 2018. At $1,650 per month, the first digital pill soon roll out to certain Medicaid patients with mental illness. Stat+. Available at: https://www.statnews.com/2018/08/30/abilify-digital-medicaid-mental-illness/

Schaefer, G. O., E. J. Emanuel, and A. Wertheimer. 2009. The obligation to participate in biomedical research. *JAMA* 302(1): 67–72. doi:10.1001/jama.2009.931

Seto, E., K. J. Leonard, C. Masino, J. A. Cafazzo, J. Barnsley, and H. J. Ross. 2010. Attitudes of heart failure patients and health care providers towards mobile phone-based remote monitoring. *Journal of Medical Internet Research* 12(4): e55. doi:10.2196/jmir.1627

Shafer, D. W., C. M. Kigin, J. J. Kaput, and G. S. Gazelle. 2002. What id digital medicine? In *Future of Health Technology*, ed. R. G. Buskop, 195–204. Amsterdam, The Netherlands: IOS Press.

Smith, A. 2017. Record shares of Americans now own smartphones, have home broadband. *FactTank* Available at: http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/

Stirratt, M. J., J. Dunbar-Jacob, H. M. Crane, et al. 2015. Self-report measures of medication adherence behavior: Recommendations on optimal use. *Translational Behavioral Medicine* 5(4): 470–482. doi:10.1007/s13142-015-0315-2

Sun, S. X., G. G. Liu, D. B. Christensen, and A. Z. Fu. 2007. Review and analysis of hospitalization costs associated with antipsychotic nonadherence in the treatment of schizophrenia in the United States. *Current Medical Research and Opinion* 23(10): 2305–2312. doi:10.1185/030079907X226050

Tandem. 2018. t:slim X2 insulin pump with Dexcom G6 CGM. Available at: https://www.tandemdiabetes.com/products/t-slim-x2-insulin-pump

Telltale heart: Pacemaker data leads to arson, fraud charges. 2017. *Fox News U.S.* Available at: http://www.foxnews.com/us/2017/02/08/police-use-data-on-mans-pacemaker-to-charge-him-with-ohio-arson.html

Thaler, R., and C. Sunstein. 2008. *Nudge: improving decisins about health, wealth and happiness*. New Haven, CT: Yale University Press.

Torous, J., and L. W. Roberts. 2017a. The ethical use of mobile health technology in clinical psychiatry. *Journal of Nervous and Mental Disease* 205(1): 4–8. doi:10.1097/NMD.0000000000000596

Torous, J., and L. W. Roberts. 2017b. Needed innovation in digital health and smartphone applications for mental health: Transparency and trust. *JAMA Psychiatry* 74(5): 437–438. doi:10.1001/jamapsychiatry.2017.0262

Yeaw, J., W. C. Lee, M. Aagren, and T. Christensen. 2012. Cost of self-monitoring of blood glucose in the United States among patients on an insulin regimen for diabetes. *Journal of Managed Care Pharmacy* 18(1): 21–32. doi:10.18553/jmcp.2012.18.1.21