THE MILBANK QUARTERLY
A MULTIDISCIPLINARY JOURNAL OF POPULATION HEALTH AND HEALTH POLICY

Original Scholarship

Ethical and Legal Implications of Remote Monitoring of Medical Devices

I. GLENN COHEN,* SARA GERKE,* and DANIEL B. KRAMER†

**Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics at Harvard Law School, Harvard University; †Richard A. and Susan F. Smith Center for Outcomes Research in Cardiology, Beth Israel Deaconess Medical Center, Harvard Medical School*

Policy Points:

- Millions of life-sustaining implantable devices collect and relay massive amounts of digital health data, increasingly by using user-downloaded smartphone applications to facilitate data relay to clinicians via manufacturer servers.
- Our analysis of health privacy laws indicates that most US patients may have little access to their own digital health data in the United States under the Health Insurance Portability and Accountability Act Privacy Rule, whereas the EU General Data Protection Regulation and the California Consumer Privacy Act grant greater access to device-collected data.
- Our normative analysis argues for consistently granting patients access to the raw data collected by their implantable devices.

Context: Millions of life-sustaining implantable devices collect and relay massive amounts of digital health data, increasingly by using user-downloaded smartphone applications to facilitate data relay to clinicians via manufacturer servers. Whether patients have either legal or normative claims to data collected by these devices, particularly in the raw, granular format beyond that summarized in their medical records, remains incompletely explored.

Methods: Using pacemakers and implantable cardioverter-defibrillators (ICDs) as a clinical model, we outline the clinical ecosystem of data collection, relay, retrieval, and documentation. We consider the legal implications of US and

The Milbank Quarterly, Vol. 98, No. 4, 2020 (pp. 1257-1289)

European privacy regulations for patient access to either summary or raw device data. Lastly, we evaluate ethical arguments for or against providing patients access to data beyond the summaries presented in medical records.

Findings: Our analysis of applicable health privacy laws indicates that US patients may have little access to their raw data collected and held by device manufacturers in the United States under the Health Insurance Portability and Accountability Act Privacy Rule, whereas the EU General Data Protection Regulation (GDPR) grants greater access to device-collected data when the processing of personal data falls under the GDPR's territorial scope. The California Consumer Privacy Act, the "little sister" of the GDPR, also grants greater rights to California residents. By contrast, our normative analysis argues for consistently granting patients access to the raw data collected by their implantable devices. Smartphone applications are increasingly involved in the collection, relay, retrieval, and documentation of these data. Therefore, we argue that smartphone user agreements are an emerging but potentially underutilized opportunity for clarifying both legal and ethical claims for device-derived data.

Conclusions: Current health privacy legislation incompletely supports patients' normative claims for access to digital health data.

Keywords: health policy, implantable cardioverter-defibrillators, pacemakers, HIPAA, GDPR.

Millions of patients live with medical devices that collect, store, and transmit health data.[1] For example, cardiac devices, including pacemakers and implantable cardioverter-defibrillators (ICDs), have dramatically expanded their diagnostic capabilities in recent years beyond the core functions of the devices themselves. Advances in sensors and storage now support data collection not only for critical device features (eg, battery life and wire performance) but also for measures of autonomic function, sleep metrics, heart failure status, and physical activity.[2-4] Similar advances have become common in noncardiac care, including devices for diabetes management and respiratory therapy, and increasingly extend even to smaller devices such as ingestible "smart pills."[5,6]

In this care model, clinicians routinely review data from patients' devices, accessible either in-office using manufacturer-specific tools or, for devices capable of connecting to remote monitoring systems, by retrieving data from websites managed by device companies. Remote monitoring has expanded sharply with the expansion of Bluetooth connectivity,

which simplifies retrieval and transfer of health data by linking patients' devices to their smartphones and manufacturer-developed applications. Some systems also can collect data from more than one device simultaneously, such as with ICD remote monitoring platforms that can also collect blood pressure measurements and weight from compatible devices.[7] This nimble, powerful, and nearly continuous data collection—often characterized as a "digital revolution"—has the potential to transform patient care for millions of patients.[8]

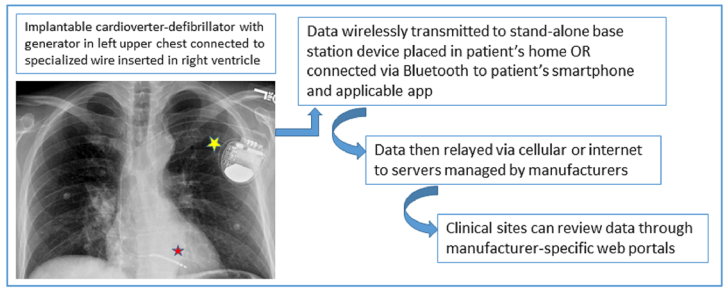
But just whose data is it? Should patients have a right to access their own data, and if so, under what circumstances? What claims do patients have for different forms of their device-collected data? How does the existing legal structure reflect or divert from our judgment about what is the most ethical way forward?

In this article, we examine the mass collection of digital health data, using the specific example of pacemakers and ICDs to illustrate the logistics of data collection, remote monitoring, and the creation of associated health care records. As a legal matter, we analyze how existing regulations in the United States and European Union apply to patient information collected by their devices and transmitted remotely to clinical providers and manufacturers. As a normative matter, we evaluate arguments addressing whether patients should have access to health data collected by their implanted devices.

Cardiac Device Basics and General Logistics of Data Collection

Most pacemakers and ICDs consist of two components, which are similar between the two device types. The first component is the lead—one or more wires that are placed in contact with the heart muscle, usually by insertion through the veins in the chest. The lead is connected to the second component, called a generator, which houses the battery, diagnostic sensors, and hardware/software components that dictate device function. Generators store device data and the components that support remote monitoring, such as radiofrequency telemetry. Pacemakers are most commonly implanted for symptomatic slow heart rhythms and, depending on patient factors, include between one and three wires that can pace different parts of the heart. ICDs are very similar, also including a lead and a generator, with their specific engineering allowing the

Figure 1. Flow of information from a patient's implantable cardioverter-defibrillator (ICD) to a clinical site via remote monitoring. The ICD system includes a wire inserted through a chest vein into the heart (red star), connected to a generator placed under the skin near the shoulder (yellow star) [Color figure can be viewed at wileyonlinelibrary.com]



device to do everything a pacemaker does with the additional capability to deliver high-voltage shocks on demand to convert sudden, dangerous heart rhythms back to normal. Figure 1 shows a typical ICD system with a lead placed inside the heart. Pacemaker and ICD features can be programmed to meet specific patient needs, such as specifying the minimum heart rate the patient will experience or defining which fast heart rhythms will trigger a shock from the ICD.

For patients with new pacemakers and ICDs implanted, the current standard of care now supports initiation of remote monitoring in one of two ways (Figure 1). Devices limited to radiofrequency communication are paired with a manufacturer-specific "base station" that the patient takes home.[9,10] This base station is usually placed in the patient's bedroom and programmed to communicate with the ICD or pacemaker once daily, often at a time when the patient is likely to be asleep. Findings that reach alert-level significance, such as a sudden change in battery function or a critical malfunction in a wire, are relayed immediately to servers maintained by manufacturers. If no alerts are identified, the servers note the timing of the last active communication between the base station and the device, which allows manufacturers and clinics to

identify whether the remote monitoring link is functioning properly, even if no alert conditions are reached.[11]

Base stations can relay their collected data in several ways but increasingly do so via cellular communication or Wi-Fi as more and more patients lack traditional landlines. If the pacemaker or ICD is Bluetooth-enabled, the base station can be replaced by installing a vendor-specific app on the patient's smartphone. The process for daily communication, data retrieval, and data transfer is similar, with an alert-driven relay of information and recording of successful communication between the smartphone and the device.

In addition to daily surveillance, most systems are configured to support scheduling of specific dates (typically every three to six months) on which a full device "interrogation" would be retrieved and sent to the manufacturer's server. This data transfer includes current measurements of battery and lead performance, arrhythmia metrics, and other diagnostic data collected by that specific device model, similar to what could be obtained at an in-office device interrogation. One key difference between in-office device evaluation and remote monitoring is that no manufacturers have pursued the ability to change the programmed parameters of a pacemaker or ICD, such as pacing functions or specific responses to detected arrhythmias, solely through remote communication. Thus, remote connectivity as currently configured can send information to clinicians, but there is no way currently for clinic sites to send information or commands in the other direction that might, for example, change any of the diagnostic or therapeutic functions of the device.

Clinical sites access data either by logging in to secure manufacturer-specific portals or by using third-party software that aggregates patient data from multiple manufacturers at once. Clinics logging in will typically be prompted to review alert-level findings, which in some clinic settings may also prompt attention by sending concurrent emails or texts to assigned clinicians. Notably, current technology allows patients to be assigned to only one clinic at a time. Similarly, clinicians who log in to vendor websites can view only their clinic's assigned patients and cannot look up information for nonassigned patients who may happen to have that brand of device.

Data Formats, Creation of Medical Records, and Research Use of Data

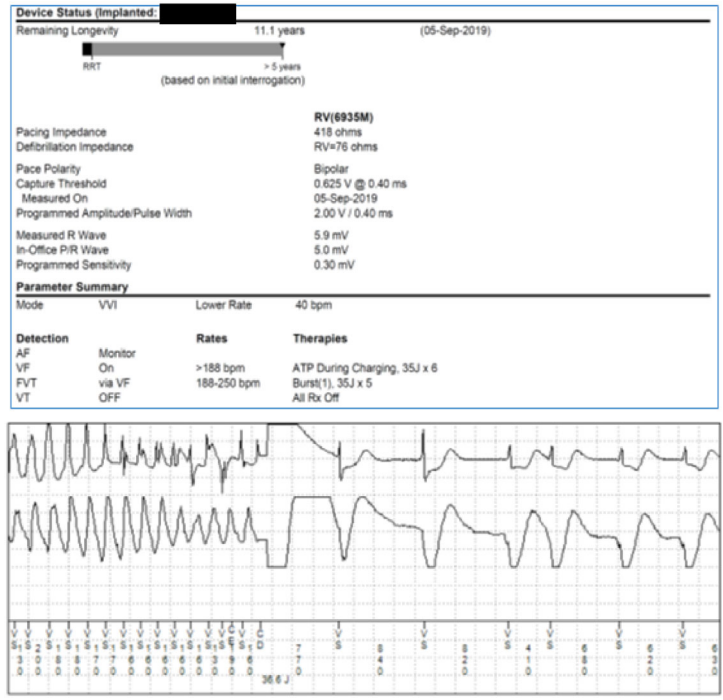
Data collected, stored, and relayed by pacemakers and ICDs exist in several formats with differing levels of detail. Clinicians review high-level summaries of battery status, wire integrity, and arrhythmia events. These summaries might include more details related to events of interest, such as the device-recorded electrograms associated with delivery of an ICD shock (Figure 2). Patient records in these portals may include all prior remote transmissions and can be exported or downloaded as summaries (eg, PDFs) by clinicians accessing these websites.

When clinicians view remote monitoring transmissions, either scheduled or alert-driven, these services may be documented in patients' medical records in several ways. For clinical use and billing purposes, at a minimum there will typically be high-level text summaries of the parameters reviewed (eg, battery life and wire function). Most electronic health record systems also allow the downloaded PDF summary from the manufacturer's website to be appended to this clinical encounter, making this part of the patient's medical record as well.

However, it is important to recognize that the devices themselves store data at a much more granular level than these summary documents. For example, physical activity information might be summarized according to hours per day over the preceding weeks or months of a patient meeting specific activity thresholds detected by the accelerometer embedded in most pacemakers and ICDs, usually with a graphical display. However, the *raw data* supporting these summaries might include additional information such as the actual activity, transthoracic impedance measures, heart rate, or other measures time-stamped minute to minute for every day of monitoring.[4] These data are encrypted and cannot be extracted, viewed, or analyzed without translation into a readable format by vendor-specific software.[2] Data transferred to manufacturers' servers generally preserve this level of detail, but this is not accessible to either clinicians or patients through routine clinical interactions.

In addition to providing clinical care, manufacturers use patient data from remote monitoring for research and development, both internally and for projects initiated by external investigators. Internally, companies can leverage data to monitor postmarket device performance and

Figure 2. Example of information gleaned from typical remote monitoring transmission from an implantable cardioverter-defibrillator. The top panel shows data regarding device characteristics including electrode measurements, battery life, and programmed parameters for pacing and high-voltage therapy. The bottom panel shows the device recording of an arrhythmia event, in this case an episode of ventricular fibrillation that was recognized by the device and treated with a high-voltage shock, after which a normal rhythm resumes. (Figure shown with patient's permission.) [Color figure can be viewed at wileyonlinelibrary.com]



evaluate the impact of iterative device changes, such as with pacing algorithms or software designed to detect lead malfunctions. Typical external research projects include those evaluating device utilization trends,[12] interactions between lead performance and battery life,[13] performance

of novel pacing algorithms,[14] or analyses that leverage physiologic data collected peripheral to core device functions.[3,4]

Patient Access to Data: Current Status

Under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, patients have generally the "right of access to inspect and obtain a copy of protected health information about … [them] in a designated record set, for as long as the protected health information is maintained in the designated record set" (45 CFR § 164.524(a)). This right can be asserted against HIPAA-covered entities (eg, most health care providers) and includes the right to direct them to transmit a copy to an entity or a designated person of the patient's choice.[15] A "designated record set" is

> a group of records maintained by or for a covered entity that is: (i) The medical records and billing records about individuals maintained by or for a covered health care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals. (45 CFR § 164.501(1))

The term *record* is defined as "any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity" (45 CFR § 164.501(2)). (For more definitions of relevant terms under HIPAA, see the section "HIPAA and Its Privacy Rule.") In general, the covered entity has 30 days to act on a patient's request for access (45 CFR § 164.524(b)(2)). The covered entity may impose a "reasonable, cost-based fee" under specific conditions, such as if the patient asks for a copy of the protected health information (45 CFR § 164.524(c)(4)).

Many covered health care providers have started to simplify this process by providing patients with internet-based portals through which they can view their own medical records in the same level of detail as any clinician accessing the same record. Millions of patients in the United States have taken advantage of these portals, such as through the OpenNotes platform, with increasing numbers of health systems adopting similar frameworks.[16] In practice, however, there are still patients who do not receive their copies upon request or receive them after a delay or

are overcharged by covered entities. Thus, the US Department of Health and Human Services Office for Civil Rights (OCR) proclaimed in early 2019 the Right of Access Initiative, promising to enforce the patients' right of access under HIPAA.[17] OCR has already put its promise into practice. In September 2019, it announced the first settlement of a case in which Bayfront Health St. Petersburg, a level II trauma and tertiary care center, agreed to pay $85,000 to OCR for a potential breach of HIPAA's right of access provision and to undertake a corrective action plan, including 12 months of monitoring by OCR.[17] In the present case, a mother requested prenatal health records about her child; she received them nine months after her initial request and only because she filed a complaint with OCR.[17] In December 2019, OCR announced the settlement of a second case under its HIPAA Right of Access Initiative.[18] This time, Korunda Medical, a Florida-based company that provides interventional pain management and comprehensive primary care to patients, failed to give a patient's medical records to a third party in electronic format.[18] As in the first case, the settlement included the payment of $85,000 to OCR for the potential breach of the right of access provision of HIPAA and a corrective action plan, including a year of monitoring.[18] These are just the first two enforcement actions taken by OCR under its Right of Access Initiative, but more are likely to come in the future. In March 2020, the Centers for Medicare and Medicaid Services (CMS) also announced the Interoperability and Patient Access final rule (CMS-9115-F), which aims to improve interoperability and give patients better access to their health information.[19]

Considering ICD/pacemaker data, different health care providers might document data gleaned from remote monitoring differently, and they may or may not choose to include the PDF summary purely for efficiency or because of idiosyncratic practice patterns, potentially limiting what patients might be able to view in portals such as the OpenNotes platform. However, even if the clinician does not make the PDF summary part of the patient's medical record, our legal assessment holds that under HIPAA's right of access provision, patients have a right to receive, upon their request, a copy of the PDF summary. In most cases, the device manufacturer will be designated a business associate under HIPAA, which imparts specific rights and responsibilities in regard to data sharing in general and the PDF summary in particular (see the section "HIPAA and Its Privacy Rule" for more detail on business associates). A HIPAA-covered entity (eg, most health care providers)

may not deny access on the grounds that the business associate maintains the protected health information (ie, the PDF summary on the manufacturer's website) requested by the patient.[15] Moreover, the PDF summary—regardless of whether it was downloaded from the website by the clinician—is used by the HIPAA-covered entity to make decisions about the individual patient and thus falls within the definition of a designated record set under HIPAA. The business associate agreement between the parties will usually govern how access requests by patients will be handled.[15] The agreement will typically contain a term stating that the ICD/pacemaker manufacturer will notify the covered health care provider promptly if the manufacturer receives any requests from a patient relating to the patient's right of access. The agreement may also explicitly remind the health care provider that the data provided are not automatically part of the patient's electronic medical records and would need to be downloaded.

A slightly different problem is that, presently, patients cannot *directly* access their own device data through any current smartphone applications provided by ICD or pacemaker manufacturers. These apps allow for data to be transmitted to clinicians, with the status of those transmissions confirmed; but with current technology the actual data are not viewable to patients and, accordingly, cannot be downloaded or transferred to any third-party health data application or software.

The US Food and Drug Administration (FDA) issued nonbinding guidance in 2017 that indicates general support for manufacturers' sharing patient-specific information from devices with patients at their request.[20] The FDA defines the term *patient-specific information* as "information unique to an individual patient or unique to that patient's treatment or diagnosis that has been recorded, stored, processed, retrieved, and/or derived from a legally marketed medical device."[20] Examples include recorded patient data, incidence of alarms, health care provider inputs regarding status and the patient's ongoing treatment, records of device failures or malfunctions, and recorded outputs such as heart rhythms and electrical activity as monitored by pacemakers.[20] The FDA also clarifies that the term *patient-specific information* does not cover any manufacturers' interpretations of data, except for data interpretations usually reported by the medical device to the patient's health care provider or the patient.[20] Moreover, the FDA correctly points out in its guidance that "sharing 'patient-specific information'

with patients upon their request may assist them in being more engaged with their healthcare providers in making sound medical decisions."[20]

But the FDA also states that "finally, this guidance does not affect any federal, state or local laws or regulations, such as … HIPAA … and the associated HIPAA Privacy Rule …, which may otherwise be applicable to the provision of patient-specific information."[20] Thus, ICD/pacemaker manufacturers may be subject to the provisions in HIPAA and the associated HIPAA Privacy Rule (see next section), and this sharing should not hamper the HIPAA standards.[21]

As a technical matter, patients also are not able to interrogate devices themselves as would be done in a clinician's office. This is because doing so requires a manufacturer-specific programmer—functionally, a modified laptop or tablet device that can communicate only with that brand of device via either radiofrequency telemetry, Bluetooth, or inductive telemetry. These devices are placed in clinics and hospitals but remain the property of their manufacturers and are not provided to patients. Among other reasons (including potential protection of trade secrets, discussed later), access to programmers is limited intentionally because incorrect usage could lead to life-threatening changes in device function. We consider later in this paper the normative question of whether patients should have access to this level of data and control over their own devices and the embedded data.

To more fully understand the legal status of patient requests for summary or raw device data, we next review the applicability of US and EU privacy laws that would govern data transfer between patients and manufacturers.

HIPAA and Its Privacy Rule

The HIPAA Privacy Rule (45 CFR Part 160 and Subparts A and E of Part 164) standards deal with the use and disclosures of "protected health information" by "covered entities" or their "business associates."[22] *Protected health information* is, in general, "individually identifiable health information" (45 CFR § 160.103). The term *individually identifiable health information* is defined as follows:

> Information that is a subset of health information, including demographic information collected from an individual, and: (1) Is created

> or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual. (45 CFR § 160.103)

HIPAA "covered entities" include health plans (eg, health insurance issuer or health maintenance organizations), health care clearinghouses (eg, billing services or repricing companies), and health care providers who transmit health information electronically in connection with particular transactions (45 CFR § 160.103). In contrast, "business associates" are organizations or persons, other than members of the workforce of a HIPAA-covered entity, that perform particular activities or tasks (eg, data analysis, processing, or administration) on behalf of such covered entity or provide specific services (eg, legal, accounting, or data aggregation) to such entity that involve the use or disclosure of protected health information (45 CFR § 160.103).[22] If a HIPAA-covered entity uses the activities or services of a business associate, the business associate contract will typically contain appropriate safeguards on the use and disclosure of protected health information (45 CFR §§ 164.502(e), 164.504(e)).

Device manufacturers could be considered HIPAA-covered entities when acting as covered health care providers, such as when the manufacturer is present in the surgery room and guides the appropriate implantation of the device.[23] However, they are much more typically designated as business associates when collecting individually identifiable health information on behalf of the HIPAA-covered entity, and there will be a business associate agreement in place.

Separate from the status of manufacturers, there is also the question of whether all data collected by manufacturers of ICDs and pacemakers are protected under HIPAA. For example, truly de-identified battery and lead performance and arrhythmia events fall outside of HIPAA. But if this health information is combined with identifiers such as the patient's name or phone number, it may become protected health information under HIPAA. All that said, in cases where device manufacturers are business associates, it seems likely that the raw data also do *not* fall within the scope of HIPAA, since clinicians or hospitals do not

hold such data.[24,25] Business associate agreements are usually limited to the data that are transferred to the clinicians or hospitals (ie, the PDF summaries).[25] Thus, ICD/pacemaker manufacturers will often likely be considered business associates under HIPAA *only* with regard to the PDF summaries and *not* regarding the raw data. However, the question of whether an ICD/pacemaker manufacturer collects the raw data on behalf of a HIPAA-covered entity, and thus falls within the definition of a business associate under HIPAA, is always to be assessed on a case-by-case basis, especially taking into account the particular business associate contract between the parties.

In the rare event that an ICD/pacemaker manufacturer is a business associate also with regard to the *raw data* under HIPAA, the patient will likely also have a right of access against the HIPAA-covered entity (ie, the health care provider) concerning the raw data. In this event, it needs to be assessed on a case-by-case basis whether the raw data are covered by the definition of a designated record set (see earlier discussion as well as 45 CFR § 164.524(a) and 45 CFR § 164.501(1)). It seems to us that, where raw data are available to them, clinicians would use the raw data (which are more detailed than the high-level PDF summaries) to make decisions about individuals. It is also worth noting in this context that the term *designated record set* has been broadly interpreted and includes clinical laboratory test reports as well as the underlying information created as part of such tests.[15,26] Thus, the right of access under HIPAA (45 CFR § 164.524(a)) likely gives individuals access to their raw data upon their request, provided the ICD/pacemaker manufacturer also collects the raw data on the covered entity's behalf and thus is considered a business associate concerning the raw data (which often will *not* be the case).

As a general rule, HIPAA-covered entities and business associates may use or disclose protected health information only if permitted or required under the HIPAA Privacy Rule (45 CFR § 164.502). Another legal avenue for accessing health information, but one that is not specific to patients, is HIPAA's privacy strategy on de-identification. *De-identified* health information "is considered not to be individually identifiable health information" under HIPAA (45 CFR § 164.502), and thus can be used and shared more freely, such as for research purposes. One option to meet the standard for de-identification under HIPAA is a determination by "a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods" (45 CFR § 164.514(b)(1)). Another option for de-identification of

protected health information is by the removal of 18 specific identifiers of the individual or of employers, household members, or relatives of the individual, such as names, medical record numbers, telephone numbers, and electronic mail addresses. The latter route is only permissible, though, if the covered entity does "not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information" (45 CFR § 164.514(b)(2)). However, many worry that the HIPAA regime is out of date for the reality of a big data world.[27-29] In particular, it seems to us that HIPAA currently does not have enough safeguards in place to give patients the right to access their raw data collected and held by manufacturers, since—in most cases—ICD/pacemaker manufacturers will likely be business associates with regard to the PDF summaries only and *not* the raw data. Other jurisdictions, such as the EU, to which we turn next, have implemented other regulatory designs.

Application of the EU General Data Protection Regulation

The EU General Data Protection Regulation (2016/679–GDPR) contains "rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data" (Art. 1(1)). *Personal data* under the GDPR are "any information relating to an identified or identifiable natural person ('data subject')" (Art. 4(1)). An *identifiable natural person* is a person "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Art. 4(1)). *Data concerning health* are "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" (Art. 4(15)). *Processing* under the GDPR is "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means," including collection, use, disclosure by transmission, storage, structuring, and erasure (Art. 4(2)).

The EU GDPR has a wide territorial scope (Art. 3). It "applies to the processing of personal data in the context of the activities of an

establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not" (Art. 3(1)). Under the GDPR, a *controller* is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" (Art. 4(7)). A *processor* is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (Art. 4(8)).

Recital 22 of the GDPR states that an "establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect." The European Data Protection Board (EDPB) has only recently, on November 12, 2019, released the second version of its guidelines on the territorial scope of the GDPR.[30] In the guidelines, the EDPB emphasizes that "the mere presence of an employee in the EU is not as such sufficient to trigger the application of the GDPR, since for the processing in question to fall within the scope of the GDPR, it must also be carried out in the context of the activities of the EU-based employee."[30] Thus, in order to establish whether Art. 3(1) of the GDPR applies, one must first determine whether a processor or controller is established in the EU, and, second, determine whether the processing of personal data is carried out "in the context of the activities of" the establishment.[30] The second step needs to be assessed on a case-by-case basis, taking into account the particular facts of the case.[30]

The EDPB mentions two factors that may help to establish whether the processing of personal data is being carried out by a processor or controller "in the context of the activities of" its establishment in the EU: (1) "Relationship between a data controller or processor outside the Union and its local establishment in the Union," and (2) "Revenue raising in the Union."[30] In particular, regarding the first factor, the EDPB clarifies that

> if a case by case analysis on the facts shows that there is an *inextricable link* between the processing of personal data carried out by a non-EU controller or processor and the activities of an EU establishment, EU law will apply to that processing by the non-EU entity, whether or not the EU establishment plays a role in that processing of data.[30] (emphasis added)

Considering medical device data, then, the GDPR thus applies in cases where the hospital or the ICD/pacemaker manufacturer is established in the EU and the processing of personal data of the patient with the ICD/pacemaker—irrespective of whether the processing takes place in the EU or outside of it—is carried out in the context of the activities of such establishment. It needs to be assessed on an individual case basis whether those criteria are met. Are personal data being processed? Are there "potential links between the activity for which the data is being processed and the activities of any presence of the organization in the Union"?[30] The nature of this link will be decisive in establishing whether the processing of personal data falls within the scope of Art. 3(1) of the GDPR.[30] It is also worth noting that the establishment of the processor or controller needs to be considered separately.[30] For example, if a hospital as a controller is established in the United States and chooses a device manufacturer as a processor in the EU, the processor's processing of personal data falls within the scope of the GDPR as per Art. 3(1). In contrast, the hospital established in the United States is not subject to the GDPR in virtue of Art. 3(1), but may fall within the scope of the GDPR as per Art. 3(2).

Art. 3(2) of the GDPR:

> applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
> (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

Under Art. 3(2)(a) of the GDPR, the offering of goods or services includes, for example, the offering of a news app or a website offering services for the creation of personalized photo albums.[30] Moreover, the offering of goods or services needs to intentionally (and not just incidentally) target data subjects in the EU.[30]

Under Art. 3(2)(b) of the GDPR, the question arises whether the GDPR applies in cases where a US patient with an ICD or pacemaker visits Germany for a holiday trip, and a processor or controller not established in the EU continues to process personal data of the patient. The EDPB clarifies that the territorial scope of the GDPR cannot be limited by the nationality or legal status of data subjects who are in the

EU[30] (see also Recital 14 of the GDPR). "Behavioral monitoring," as per Art. 3(2)(b) of the GDPR, for example, can be carried out through the tracking of an individual on the internet or through wearables or other smart devices.[30] In the view of the EDPB, behavioral monitoring encompasses a wide range of activities, including the "monitoring or regular reporting on an individual's health status."[30] However, the board also emphasizes "that the fact of processing personal data of an individual in the Union alone is not sufficient to trigger the application of the GDPR to processing activities of a controller or processor not established in the Union. The element of 'targeting' individuals in the EU … by monitoring their behaviour … must always be present in addition."[30]

Thus, in the previous example, while the behavior of the US patient with an ICD or pacemaker who visits Germany for a holiday trip will continue to be monitored, the behavioral monitoring is not "'targeting' individuals in the EU," but is only directed at patients in the United States. Hence, the processing of personal data by the processor or controller not established in the EU falls outside the scope of the GDPR. The GDPR would apply only if the processor or controller not established in the EU targeted the behavioral monitoring of patients in the EU.

In summary, in our view, under Art. 3(1), the GDPR applies to the processing of personal data of US patients by a US hospital or US ICD/pacemaker manufacturer when there is an *inextricable link* between the processing that takes place in the United States and the activities of a local establishment in the EU (eg, a branch in Germany) of that hospital or manufacturer. However, for many US hospitals and US ICD/pacemaker manufacturers that maintain a local establishment in the EU, the processing of personal data of US patients will likely not be "in the context of the activities of" that establishment, and thus the GDPR will not apply as per Art. 3(1). In general, these cases must be decided on a case-by-case basis.

Under Art. 3(1), the GDPR also applies, for example, to a device manufacturer's processing of personal data of US patients when the hospital is established in the United States (and does not have any stable arrangement in the EU) and chooses a device manufacturer that is exclusively established in the EU.

US hospitals and US ICD/pacemaker manufacturers may be subject to the GDPR as per Art. 3(2) in cases where the processing activities are related to "the offering of goods or services" to data subjects who are in the EU or "the monitoring of their behaviour as far as their behaviour takes place within the Union." However, the GDPR does *not* apply in cases where a device manufacturer is clearly *not* established in the EU and continues to process data from a US patient with an ICD or pacemaker who is on a holiday trip in Germany, since the behavioral monitoring is targeting individuals in the United States and not in the EU.

In cases where a data controller or a processor is subject to the GDPR, the relevant requirements should be fulfilled to avoid administrative fines up to 20 million euros or up to 4% of a company's total global annual turnover of the previous financial year (Art. 83 of the GDPR). For example, data subjects have rights pursuant to Arts. 12 to 22 of the GDPR against the controller. In particular, it seems to us that the GDPR generally also gives patients the right to receive the raw data from the controller. In the context of Art. 20 of the GDPR (ie, the right to data portability), the Data Protection Working Party explicitly mentions in its guidelines that the right to data portability "may also include other raw data such as the heartbeat tracked by a wearable device."[31] The right of data portability complements the right of access under Art. 15 of the GDPR.[31] Art. 20(1) of the GDPR states that the personal data concerning the data subject should be received "in a structured, commonly used and machine-readable format." The Data Protection Working Party's guidelines also clarify that "where the personal data requested are processed by a data processor, the contract concluded in accordance with Article 28 of the GDPR must include the obligation to assist 'the controller by appropriate technical and organizational measures, … to respond to requests for exercising the data subject's rights.'"[31]

The California Consumer Privacy Act

Although there is currently no US federal privacy law in sight, US states have started to take action to better protect consumers' data privacy. On January 1, 2020, the California Consumer Privacy Act (CCPA) became effective. The CCPA—the "little sister" of the GDPR—grants several rights to consumers (ie, natural persons who are California residents; see

Cal. Civ. Code § 1798.140(g)) concerning their personal information that is held by certain businesses. *Personal information* is "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household" (Cal. Civ. Code § 1798.140(o)(1)). Examples include identifiers such as a postal address, a real name, and an email address, as well as biometric information and geolocation data (Cal. Civ. Code § 1798.140(o)(1)). Personal information also includes "inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes" (Cal. Civ. Code § 1798.140(o)(1)(K)). It does not mean publicly available information—"information that is lawfully made available from federal, state, or local government records" (Cal. Civ. Code § 1798.140(o)(2)).

Business under the CCPA is defined as follows:

> (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the *profit or financial benefit* of its shareholders or other owners that *collects consumers' personal information* or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does *business in the State of California*, and that satisfies one or more of the following thresholds:
> (A) Has annual *gross revenues in excess of twenty-five million dollars* ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.
> (B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, *the personal information of 50,000 or more consumers, households, or devices*.
> (C) Derives *50 percent or more of its annual revenues from selling consumers' personal information*.
> (2) Any entity that controls or is controlled by a business as defined in paragraph (1) and that shares common branding with the business. (emphasis added) (Cal. Civ. Code § 1798.140(c))

Thus, the CCPA has a broad scope and covers some of the data that are not covered by HIPAA. It is also essential to note that the CCPA does not apply to protected health information that is collected by covered entities or their business associates under HIPAA (Cal. Civ. Code § 1798.145(c)(1)(A)).

Considering ICDs and pacemakers, as mentioned previously, most device manufacturers will likely not be considered business associates under HIPAA in regard to the raw data. But it might well be that at least California residents have a right against device manufacturers under the CCPA to access their raw data as well as a right to data portability. As mentioned, the CCPA grants several rights to California residents. In particular, under § 1798.100(a), "a consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected." The term *collects* is defined as "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior" (Cal. Civ. Code § 1798.140(e)). Thus, it seems to us that this definition also includes raw data collected by ICDs or pacemakers, since the manufacturers receive information from the consumer passively via the device. Moreover, the raw data are also considered personal information under the CCPA as long as the raw data are, for example, combined with identifiers such as the patient's name. Moreover, the CCPA states that if a business "receives a verifiable consumer request from a consumer to access personal information," it

> shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance. (Cal. Civ. Code § 1798.100(d))

Since the act is so new, there is still a lot of uncertainty regarding the scope of its rights. Thus, it is recommended that the attorney general's regulations explicitly clarify whether the raw data linked with identifiers are covered by the CCPA.

The preceding discussion argues that (1) HIPAA supports access of individuals to inspect and obtain a copy of protected health information; (2) even if the clinician does not make the PDF summary part of the patient's medical record, patients, upon their request, have a right to receive a copy of the PDF summary under HIPAA's right of access provision; (3) in cases where device manufacturers are business associates, the

raw data likely do not fall within the scope of HIPAA; (4) the EU GDPR may apply under specific conditions to US hospitals and device manufacturers; (5) the GDPR generally also gives patients the right to receive the raw data from the controller; (6) the CCPA provides additional privacy protections for California residents; (7) the CCPA does not apply to protected health information that is collected by covered entities or their business associates under HIPAA; and (8) the CCPA may give California residents a right against device manufacturers to access their raw data as well as a right to data portability.

What Do Patients Agree To? User Agreements for Remote Monitoring for Hospital-Based Products

All that said, an important finding is that in many cases, patients currently do not have a legal right of access to their raw device data. This state of affairs might surprise many patients—data generated by and about them that may be relevant to their health might be inaccessible to them, despite the general thrust of laws like HIPAA giving patients significant rights to access their data.

Is this a state of affairs that patients agreed to? It appears largely no. Patients enrolled in remote monitoring do not typically provide signed informed consent specifically for this aspect of their clinical care. Rather, the terms of use for their remote monitoring system are governed by contracts between the manufacturer and their clinical site. For example, one author works at an academic medical center in the United States with an ambulatory device clinic that monitors approximately 2,000 patients across four manufacturers (Medtronic, Boston Scientific, Abbott, and Biotronik). With each of these manufacturers, the medical center has a business associate contract that defines terms of use for the remote monitoring platforms specific to each vendor. However, these documents are confidential and cannot be reviewed by external parties. Ideally, several aspects of these contracts would be publicly knowable by patients, such as (1) specific articulation of patient access rights to collected data; (2) use of data for research, development, or marketing; and (3) cybersecurity and privacy protections. There is no signed user agreement associated with the use of home-based remote monitoring systems, and participation is wholly opt-in or opt-out with no provisions for patients

to selectively participate. Therefore, patients are the subjects of contracts regarding patient data that they not only did not agree to, but may not even be able to view and certainly not to alter.

We also note an important observation about apparently arbitrary differences in patients' access to their device data. Based on our interpretation of the GDPR, whether patients have a valid legal claim to the raw data from their devices may depend in part on which brand of device they receive and whether that manufacturer is subject to the GDPR's jurisdiction. Patients generally do not have much influence over what brand of pacemaker or ICD they receive, as these decisions are generally made by the implanting physician. Physicians select devices based on a variety of factors that include anatomic considerations (eg, some ICDs are shaped differently and may be better suited to some patients than others), clinical features (eg, whether a given ICD is compatible with magnetic resonance imaging), and contracting between the vendors and the implanting institution. Moreover, California residents who have ICDs and pacemakers are currently better off than other patients in the United States concerning access to their device data.

User Agreements for Remote Monitoring for Smartphone-Based Monitoring

The patient privacy, control, and information ecosystem becomes more complicated for smartphone-based products for remote monitoring. Presently only a few apps are available in the United States for both Mac OS and Android systems, but this technology is likely to become more common in the near future. Smartphones are appealing clinically as the relay station for remote monitoring because of their ubiquity and nimble connectivity. Patients commonly experience symptoms or develop subclinical but important findings while away from their base stations. Smartphone-enabled data relay may avoid unnecessary emergency room visits or facilitate necessary care more promptly than would otherwise be achievable.

Transitioning toward smartphone apps is also attractive to manufacturers. Vendors who provide cellular-enabled base stations are responsible for those monthly charges, whereas with smartphone apps those costs are transferred to patients. Smartphones also provide

streamlined pathways for software updates and, depending on the design and settings of each app, may facilitate data collection for a wide array of uses.

Although a full comparison of the user agreements of all smartphone-based applications marketed in the United States related to pacemaker or ICD remote monitoring on the Apple App Store and Google Play App Store for Android is beyond the scope of this paper, we do make the following observations based on the nature of these agreements in general: In contrast to the hospital-based arrangements, these user agreements are fully available to patients for review as prospective users, albeit in the somewhat opaque and overwhelming language of most app user agreements.[32] These agreements would theoretically provide a platform, then, for patients to understand aspects of their relationship with the manufacturer, including data access and portability and the use of their data for research or provision of those data by manufacturers to third parties (whether de-identified or not).

In addition, apps' presence on patients' smartphones contrasts with home-based monitoring because of the need for clear delineation of permissions—what other apps or smartphone data does this remote monitoring app have access to? GPS-tagged location information, for example, may be of interest to manufacturers and even germane to their understanding of device and app function according to cellular and Wi-Fi coverage. Theoretically, granting access to a contact list might enable an app to notify family members or selected proxies in cases of emergencies. However, apparently reasonable connections between a remote monitoring app and other phone functions will necessarily require close scrutiny regarding unintended uses of these additional data, and whether patients have access to these integrated health data that they themselves are essential for creating.

Ethical Considerations for Patient Access to Data

Even taking as given the legal regimes just discussed, there is a separate ethical question of whether patients *should* have access to data—whether in summary or raw format—generated by their devices and stored either in the devices themselves or collected elsewhere through remote monitoring. Even if the law did not mandate such access, nothing would stop

hospital systems or manufacturers from enabling such access for ethical reasons. Furthermore, if the ethical reasons were weighty enough, they may justify changes to the legal regime to impose access obligations.

To be sure, patients usually *do* have access to data aggregated in designated record sets such as medical records. But as described earlier, pacemakers and ICDs collect data and relay the data to industry servers via remote monitoring, more frequently and in more granular detail than would be reflected in most electronic health record systems. For example, even a very diligent clinical site might only document summary device-derived findings monthly or every three to six months. If patients want more frequent or more detailed data (such as daily measurements of physiologic parameters or arrhythmia burden), should clinics or manufacturers make these available?

It is worth considering first *why* patients might want data with this higher level of detail. (Note that we are unaware of empirical studies evaluating whether actual heart rhythm device patients commonly do, in fact, want this access.) First, there are several clinical scenarios in which patients might be interested in accessing their device data directly. Many patients with cardiac devices have conditions, such as congestive heart failure or atrial fibrillation, for which daily physiologic measurements may be clinically important. Patients commonly titrate medication use, such as diuretics or rate control agents, to physiologic parameters (eg, weight, heart rate). Modern pacemakers and ICDs capture metrics of heart failure, such as transthoracic impedance, physical activity, and heart rate variability, that may be of interest to patients as part of their own management of their chronic disease. Pilot studies involving daily review of arrhythmia burden to inform the use of anticoagulation management have demonstrated potential clinical benefits from more frequent data review than would be typically performed in routine care.[33,34] Similar studies have used intensive review of remote monitoring data in heart failure patients to improve clinical outcomes.[35] A key barrier to widespread implementation, however, is the need for clinician review of device data. As current smartphone apps and internet portals for remote monitoring data do not give patients access to their own data, enabling patients to do so may broaden the applicability of these management strategies. Some patients may also find these data of interest more informally, for example, in order to correlate daily experiences such as dietary changes with device-collected data, or to look for findings potentially related to symptoms such as palpitations.

As described previously, devices also often collect data with daily or minute-to-minute time-stamping that can facilitate more complex analytics.[2] Even to clinicians, however, this level of data is encrypted and not accessible without manufacturer assistance, and despite anecdotal reports of patients requesting this level of data access, we are not aware of this actually occurring. Patients might be interested in this degree of detail in order to integrate device-derived data with those collected from other wellness trackers, for example, or for conducting their own research. Patients with frequent but nonspecific symptoms (such as palpitations) may wish to correlate their experiences with device-related data more frequently than they would want to mediate through their clinicians, whether out of embarrassment or convenience or for economic reasons. The economic concern is particularly salient, as depending on patient insurance they may be responsible for copayments or charges associated with physician review of remote monitoring transmissions, even if in some cases the patients could answer the clinical question themselves simply by reviewing their own data.

For many patients, data access thus derives from an interest in managing their own health care, in some cases with a level of urgency or attention that would be impractical otherwise. Thus, we find a strong argument from respect for patient autonomy in favor of providing patients greater access to their device data. While the aforementioned scenarios might be reasons why patients would want access, their right to self-determination, ownership over their own physiology, and opportunity to participate fully in their own health maintenance weigh heavily in favor of providing access. In practice, this would mean redesigning both smartphone applications and web portals to allow patients access similar to or beyond what clinicians review. Moreover, we have noted already that existing access to device data depends in part on the way in which those data are reported in patients' medical records, which may vary according to provider or health system. This variability itself supports our claim that patients ought to have access to their own data, as doing so may help reduce or eliminate otherwise random or systematic disparities in the quality and quantity of data available for their own review.

There are several potential arguments against enabling patients to better manage their own health, which we consider in turn here. First, manufacturers might argue that the complexity of the underlying data justifies restricting access, as patients lack the requisite training to

properly interpret device data. Common arguments against patient access often start with the observation that device-derived data are voluminous, frequently technical, and clinically nuanced beyond other forms of health data (eg, laboratory testing with straightforward reference values for "normal"). Restricting patient access can therefore be viewed through a lens of benign paternalism that seeks to shield patients from unnecessary worry, concern, or confusion. We disagree. There does not seem to be any substantive difference between data collected by devices, or collected and stored by remote monitoring, and other forms of health care data such as lab tests or radiology. Notably, those data (eg, patient imaging) may also be complex or require clinical knowledge for interpretation, but are still routinely available to patients. Improved patient access to data has not caused major problems in those areas, so we are skeptical of arguments that this area is so different as to justify such a different regime. Indeed, one benefit of patients reviewing their own laboratory data or radiology reports is that this provides another layer of assurance that important findings are not missed. This may be even more compelling for device-recorded data, which accumulate at the clinical level so rapidly that human or system errors are inevitable. Even if a particular patient never looks at the data, knowing they could access the data if they wanted and that they are viewed by their physician as a partner in their own health, and not a "subject" to be managed, can have important benefits for instilling trust.

A second, more technical concern is whether giving patients access via their smartphones or personal computers introduces cybersecurity risks, particularly in settings without hospital-level information technology infrastructure. For example, if patients use public Wi-Fi or unencrypted computing systems to access their device data, those data and the systems in which they are stored may be more vulnerable to exposure than is currently the case. These data access issues may intersect with cybersecurity risks related to wireless data transmissions insofar as manufacturers do take steps to protect device data and the security of data relay that might complicate patient access. Such cybersecurity risks argue for restricting access, grounded in the ethical principle of nonmaleficence. But not all forms of access raise the same level of cybersecurity risk. For some access regimes the increased risk of malicious data interception or hacking is minimal, while in others there is a genuine trade-off between ethical principles of nonmaleficence and patient autonomy. What is important is not to allow "cybersecurity" to become an opportunistic magic word

that restricts all forms of access. There should be a presumption in favor of patients' access to their own data, a presumption that the makers of devices can overcome by showing both significant cybersecurity risks and the absence of reasonable alternative designs that could both enable patient access and protect data security. For example, manufacturers might limit patient access to data when the app is accessed on public networks, or require multifactor authentication to ensure that access is provided only to authorized persons. But cybersecurity as a blanket worry does not, in our view, overturn the overall assessment that patients should have access to their device data.

Lastly, though for understandable reasons not typically articulated by the makers of these devices, there may also be concerns that some forms of patient access might undermine the commercial interests and the protection of trade secrets of the hardware makers.[24] One set of concerns is about competitor behavior, in particular that competitors might use information generated by patients to develop their own products and undermine the device maker's own market share. For example, under HIPAA, a covered entity does not need to give access to protected health information if this requires disclosure of confidential commercial information or trade secrets (sec. 1172(e)).[36] This principle could also be applied to cases where raw data are not covered by HIPAA. Although pacemakers and ICD functions are generally similar across vendors, some algorithms and device features are proprietary and provide some measure of competitive advantage.

However, in the case of giving individual patients access to their individual data, the worry seems slight—it will be hard to generate a robust database of enough patients' data to really change the competition landscape and to compromise manufacturers; moreover, even if this came about, it is possible that other types of intellectual property protections such as patents would serve as a bulwark. A different concern has more to do with the possibility that if enough patients shared their data with researchers, the data analysis might show shortcomings in the devices themselves. But if existing devices are not working as designed or the design leads to problematic outcomes that become manifest from analyzing the so-far secret data, far from a problem there may be an affirmative public health reason for making these data available.

This raises a closely related objection to releasing raw data, specifically potential fears of liability claims, applied to either manufacturers or clinicians. For example, patients' review of their own raw device data

might identify deficiencies in algorithms designed to detect rapid battery depletion, interpret arrhythmias, or deliver high-voltage therapy. These findings theoretically could expose manufacturers to liability. Similarly, patients might use raw device data to assess clinicians' review and management of remote monitoring information. As with trade secrets, however, the possibility that actual technical or clinical errors might be identified does not provide an ethical argument against sharing those data with patients.

One important issue brought to light by this discussion is that access may not be enough. Instead, what is needed is access and *portability*, such as the right of access under Art. 15 and the right to data portability under Art. 20 of the GDPR. Here, data derived from consumer wearable devices provide a useful analog, as many of these devices allow for export of raw data toward third-party software (eg, data from a GPS-enabled multisport watch from one vendor can be loaded into websites such as Strava or other fitness programs). Granting patients access to their own data may provide some sense of empowerment around "ownership" of these data insofar as it becomes literally transferable and under patient control. We further emphasize that in contrast to the legal analysis, there is no important ethical distinction between providing patients with access to their summary versus raw device data.

Summary Observations

Data collection by implantable devices such as pacemakers and ICDs provides extraordinary windows into patients' health. Current systems are well integrated into cardiovascular care and will increasingly impact more and more disease areas. Yet this technological power may have outpaced its governance, leaving uncertainty about the way in which health privacy laws in the United States or EU apply to different forms of digital health data. Our analysis reinforces prior observations that digital health data collection forces close scrutiny of patient privacy, data rights, and access in both legal and ethical terms. We find that HIPAA's Privacy Rule supports patient access to summary data but in most cases does not provide patients with a right to access their raw data. By contrast, the EU GDPR has a broad scope and gives data subjects more expansive rights, including generally the right to receive their raw data from the controller. This places new scrutiny on the brand of device patients receive, as the relationship of that corporate entity and its data-processing

activities to the territorial EU may have implications as to which privacy regulations apply. It also seems likely that the CCPA grants California residents a right against device manufacturers to access their raw data as well as a right to data portability. Moreover, as smartphones increasingly become part of the ecosystem for digital health data collection, associated user agreements provide an underutilized opportunity to clarify data access while also clearly circumscribing the nature of the health data being collected in relation to other smartphone-derived information.

Lastly, our ethical analysis of arguments regarding patient access supports granting patients the right to access both summary *and* raw data from their device. For US patients certainly, and possibly EU patients, our normative conclusions, therefore, highlight an area of tension between what patients ought to be able to do with data collected from within their bodies and what current privacy laws and the practice support.

References

1. Kramer DB, Fu K. Cybersecurity concerns and medical devices: lessons from a pacemaker advisory. *JAMA*. 2017;318(21):2077-2078.
2. Kramer DB, Tsai T, Natarajan P, Tewksbury E, Mitchell SL, Travison TG. Frailty, physical activity, and mobility in patients with cardiac implantable electrical devices. *J Am Heart Assoc*. 2017;6(2).
3. Kramer DB, Jones PW, Rogers T, Mitchell SL, Reynolds MR. Patterns of physical activity and survival following cardiac resynchronization therapy implantation: the ALTITUDE activity study. *Europace*. 2017;19(11):1841-1847.
4. Kramer DB, Mitchell SL, Monteiro J, et al. Patient activity and survival following implantable cardioverter-defibrillator implantation: the ALTITUDE activity study. *J Am Heart Assoc*. 2015;4(5).
5. Aripiprazole with digital ingestion tracking (Abilify MyCite). *Med Lett Drugs Ther*. 2019;61(1564):15-16.
6. Gerke S, Minssen T, Yu H, Cohen IG. Ethical and legal issues of ingestible electronic sensors. *Nat Electron*. 2019;2:329-334.
7. LATITUDE NXT Remote Patient Monitoring System wireless weight scale and blood pressure monitor. Boston Scientific website. https://www.bostonscientific.com/en-US/products/remote-patient-monitoring/latitude-nxt.html. Accessed November 29, 2019.

8. Topol EJ. *The Creative Destruction of Medicine: How the Digital Revolution Will Create Better Health Care*. New York: Basic Books; 2013.
9. Slotwiner D, Varma N, Akar JG, et al. HRS Expert Consensus Statement on remote interrogation and monitoring for cardiovascular implantable electronic devices. *Heart Rhythm*. 2015;12(7):e69-100.
10. Zeitler EP, Piccini JP. Remote monitoring of cardiac implantable electronic devices (CIED). *Trends Cardiovasc Med*. 2016;26(6):568-577.
11. Ploux S, Varma N, Strik M, Lazarus A, Bordachar P. Optimizing implantable cardioverter-defibrillator remote monitoring: a practical guide. *JACC Clin Electrophysiol*. 2017;3(4):315-328.
12. Hsu JC, Saxon LA, Jones PW, Wehrenberg S, Marcus GM. Utilization trends and clinical outcomes in patients implanted with a single- vs a dual-coil implantable cardioverter-defibrillator lead: insights from the ALTITUDE study. *Heart Rhythm*. 2015;12(8):1770-1775.
13. Steinhaus DA, Waks JW, Collins R, Kleckner K, Kramer DB, Zimetbaum PJ. Effect of smaller left ventricular capture threshold safety margins to improve device longevity in recipients of cardiac resynchronization-defibrillation therapy. *Am J Cardiol*. 2015;116(1):85-87.
14. Hsu JC, Birnie D, Stadler RW, Cerkvenik J, Feld GK, Birgersdotter-Green U. Adaptive cardiac resynchronization therapy is associated with decreased risk of incident atrial fibrillation compared to standard biventricular pacing: a real-world analysis of 37,450 patients followed by remote monitoring. *Heart Rhythm*. 2019;16(7):983-989.
15. Individuals' right under HIPAA to access their health information 45 CFR § 164.524. US Department of Health and Human Services website. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html. Last reviewed January 2020. Accessed February 2, 2020.
16. Esch T, Mejilla R, Anselmo M, Podtschaske B, Delbanco T, Walker J. Engaging patients through open notes: an evaluation using mixed methods. *BMJ Open*. 2016;6(1):e010034.
17. US Department of Health and Human Services. OCR settles first case in HIPAA Right of Access Initiative. Press release. September 9, 2019. https://www.hhs.gov/about/news/2019/09/09/ocr-settles-first-case-hipaa-right-access-initiative.html. Accessed February 2, 2020.
18. US Department of Health and Human Services. OCR settles second case in HIPAA Right of Access Initiative. Press release.

December 12, 2019. https://www.hhs.gov/about/news/2019/12/12/ocr-settles-second-case-in-hipaa-right-of-access-initiative.html. Accessed February 2, 2020.

19. Interoperability and patient access fact sheet. Centers for Medicare and Medicaid Services website. https://www.cms.gov/newsroom/fact-sheets/interoperability-and-patient-access-fact-sheet. Published March 9, 2020. Accessed June 18, 2020.
20. US Food and Drug Administration. *Manufacturers Sharing Patient-Specific Information from Medical Devices Upon Request: Guidance for Industry and Food and Drug Administration Staff*. Silver Spring, MD: US Food and Drug Administration; 2017. https://www.fda.gov/media/98519/download. Accessed August 30, 2019.
21. Medical device HIPAA compliance: sharing patient information. The Compliancy Group website. https://compliancy-group.com/medical-device-hipaa-compliance-sharing-patient-information/. Accessed February 2, 2020.
22. US Department of Health and Human Services. *OCR Privacy Brief: Summary of the HIPAA Privacy Rule*. Washington, DC: US Department of Health and Human Services; 2003. https://www.hhs.gov/sites/default/files/privacysummary.pdf. Accessed November 29, 2019.
23. When may a covered health care provider disclose protected health information, without an authorization or business associate agreement, to a medical device company representative? US Department of Health and Human Services website. https://www.hhs.gov/hipaa/for-professionals/faq/490/when-may-a-covered-health-care-provider-disclose-protected-health-information-without-authorization/index.html. Published February 4, 2004. Accessed November 29, 2019.
24. Rowe E. Sharing data. *Iowa Law Rev*. 2018;104(1):287-323.
25. Marcus AD, Weaver C. Heart gadgets test privacy laws. *Wall Street Journal*. November 28, 2012. https://www.wsj.com/articles/SB10001424052970203937004578078820874744076. Accessed December 16, 2019.
26. Barnes M, Stayn S, Forster D, Russell-Einhorn M, Peloquin D, Medina-Jordan A. The CLIA/HIPAA conundrum of returning test results to research participants. *Medical Research Law and Policy Report*. July 15, 2015. https://www.ropesgray.com/~/media/Files/articles/2015/July/2015-07-15-Bloomberg-BNA.ashx. Accessed February 2, 2020.
27. Cohen IG, Mello MM. Big data, big tech, and protecting patient privacy. *JAMA*. 2019; 322(12):1141-1142.
28. Price WN II, Cohen IG. Privacy in the age of medical big data. *Nat Med*. 2019;25(1):37-43.

29. Cohen IG, Mello MM. HIPAA and protecting health information in the 21st century. *JAMA*. 2018;320(3):231-232.
30. European Data Protection Board. *Guidelines on the Territorial Scope of the GDPR, 2018*. Brussels, Belgium: European Data Protection Board; 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf. Accessed December 9, 2019.
31. Right to data portability. European Data Protection Board website. https://edpb.europa.eu/our-work-tools/our-documents/guideline/right-data-portability_en. Published May 25, 2018. Accessed December 16, 2019.
32. Huckvale K, Torous J, Larsen ME. Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. *JAMA Netw Open*. 2019;2(4):e1925 42.
33. Waks JW, Passman RS, Matos J, et al. Intermittent anticoagulation guided by continuous atrial fibrillation burden monitoring using dual-chamber pacemakers and implantable cardioverter-defibrillators: results from the Tailored Anticoagulation for Non-Continuous Atrial Fibrillation (TACTIC-AF) pilot study. *Heart Rhythm*. 2018;15(11):1601-1607.
34. Passman R, Leong-Sit P, Andrei AC, etal. Targeted anticoagulation for atrial fibrillation guided by continuous rhythm assessment with an insertable cardiac monitor: the Rhythm Evaluation for Anticoagulation With Continuous Monitoring (REACT.COM) pilot study. *J Cardiovasc Electrophysiol*. 2016;27(3):264-270.
35. Hindricks G, Taborsky M, Glikson M, et al. Implant-based multiparameter telemonitoring of patients with heart failure (IN-TIME): a randomised controlled trial. *Lancet*. 2014;384(9943):583-590.
36. Steirs W. Policy on release of "raw data" from psychological and neuropsychological testing. Association of Psychology and Postdoctoral Internship Centers. https://www.appic.org/Portals/0/docs/Rawdata_Steirs_7-10-05.doc. Accessed December 16, 2019.

Funding/Support: DBK is supported by the Greenwall Faculty Scholars Program. SG and IGC were supported by a grant from the Collaborative Research Program for Biomedical Innovation Law, a scientifically independent collaborative research program supported by a Novo Nordisk Foundation grant (NNF17SA0027784). IGC also was supported by the Harvard Catalyst Clinical and Translational Science Center.

Conflict of Interest Disclosures: All authors completed the ICMJE Form for Disclosure of Potential Conflicts of Interest. IGC has served as a bioethics consultant

for Otsuka Pharmaceutical on its Abilify MyCite product. The company neither funded the preparation of this manuscript nor played a role in its drafting or review. SG received funding from the German Federal Ministry of Education and Research, from April 1, 2016, to March 31, 2018, outside the submitted work.

Acknowledgments: We thank David J. Peloquin at Ropes & Gray LLP for his review of data privacy laws.

Address correspondence to: Daniel B. Kramer, MD, MPH, Beth Israel Deaconess Medical Center, Harvard Medical School, 375 Longwood Ave, 4th Floor, Boston, MA 02215 (email: dkramer@bidmc.harvard.edu).