Sharing Data

Elizabeth A. Rowe[*]

ABSTRACT: This Article examines a major challenge related to the Internet of Things: the sharing of data, as presented in the context of medical software. In particular, it examines the tensions between manufacturers and patients with respect to access to data generated from implantable medical devices. Patients argue that they do not have sufficient access to the data, and they do not control what could happen to the information collected from their devices. While manufacturers recognize that patients have some right to access their own medical data, they do not believe it outweighs their intellectual property rights in controlling access to the information.

The Article recommends a disclosure spectrum from which to frame the sharing of information, one that takes a nuanced approach to what might be shared. Determining how and what to share is challenging, and the Article suggests a closer inquiry into the nature and scope of the data requested in arriving at an appropriate response. This framework for thinking about how to balance data access rights, might also be useful more generally, as we continue to face similar questions with other interconnected devices in the Internet of Things.

---

[*] Irving Cypen Professor of Law, Distinguished Teaching Scholar, and Director, Program in Intellectual Property Law, University of Florida Levin College of Law. I express my appreciation to Andrea Matwyshyn, Kenneth Nunn, Sharon Sandeen, Christopher Seaman, Felix Wu, participants at a Washington & Lee School of Law faculty workshop, and the Cardozo School of Law IPIL Colloquium for insights, comments, or conversations about the ideas expressed in earlier versions of this work. Thank you to Janelle Elysee, Giulia Farrior, Corey Parker, Christopher Shand, and Eric VanWiltenburg for excellent research assistance, and to the University of Florida Levin College of Law for its research support.

I. INTRODUCTION

In the early morning hours last September, Ross Compton awoke to the sound of an explosion, followed by intense smoke and flames in his Ohio home.[1] He was unable to find his phone to call 911, until he heard it ringing. It was his alarm company responding to his fire alarm. After speaking with them, Mr. Compton then called 911 for help, while laboring to breathe and speak. As the fire trucks made their way to his home, Mr. Compton, who uses an external heart pump and an implantable pacemaker, broke the glass of his bedroom window. He slid his medical equipment to the window and threw them outside, along with some other items. He survived the fire. A few months later, using the data from his implantable pacemaker, and in what is believed to be a case of first impression, Mr. Compton was indicted on charges of arson and insurance fraud, and the judge refused to suppress the evidence.[2] This story highlights an important irony related to intellectual property law and

1. This story is based on Motion to Suppress, State v. Compton, CR 2016 12 1826 (Ohio Ct. C.P. Butler Cty. May 5, 2017).

2. Chris Matyszczyk, *Judge Rules Pacemaker Data Can Be Used Against Defendant*, CNET (Jul. 12, 2017, 7:32 PM), https://www.cnet.com/news/judge-rules-pacemaker-data-can-be-used-against-defendant.

policy: While a patient himself does not have direct access to the data generated by the implantable medical device in his body, that very information may be accessible to others, including the government, and can be used against him.

Implantable medical devices have changed the lives of millions of Americans who use them to monitor and treat such health conditions as cardiac arrhythmias, diabetes, and other serious conditions. Examples of implantable medical devices include pacemakers, implantable defibrillators, insulin pumps, and continuous glucose monitors.[3] They measure such things as electric cardiac activity, temperature, physical motion, and other clinical data points.[4] These devices measure and record data about the physiological development in a patient's body, and communicate that data wirelessly to a monitoring system.[5] These monitoring systems may then transmit the data to the hospital and then to the physician overseeing the patient's care.[6] In order for the patient to obtain information from the device, however, she would typically need to visit the physician's office or hospital. Herein lies the problem.

Patients and patient advocates have argued that information that is critical to a patient's care and located within an implantable device is often not available to the patient.[7] For instance,

> [s]ometimes the symptoms of things, such as a cardiac event, can be indistinguishable from other day to day occurrences, such as dizziness or fatigue. If I'm dizzy, I'm not going to be sure if I have allergies, I missed breakfast, or I'm having a cardiac episode. My device knows but in many cases it wouldn't necessarily let me know.[8]

In other words, the device, even though it is recording heart activity all the time, may not share that information with the patient, and the patient will not have the information until he goes in for a checkup. [9] As a result, some patients have resorted to taking matters into their own hands, hacking into

3. *See, e.g.*, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65,944, 65,955 (Oct. 28, 2015) (codified at 37 C.F.R. § 201.40 (2017)).

4. Method & Apparatus for Enabling Data Commc'n Between an Implantable Med. Device and a Patient Mgmt. Sys., U.S. Patent No. 7,127,300 (filed Dec. 23, 2002) (issued Oct. 24, 2006).

5. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. at 65,958.

6. *Id.*

7. U.S. COPYRIGHT OFFICE, SIXTH TRIENNIAL 1201 RULEMAKING HEARINGS 17 (May 29, 2015), https://www.copyright.gov/1201/2015/hearing-transcripts/1201-Rulemaking-Public-Roundtable-05-29-2015.pdf.

8. *Id.* at 17–18.

9. *Id.* at 24.

their machines in order to receive real-time data about their care and treatment.[10]

While the manufacturers of these devices concede that patients have some right to access their own medical data, they believe that the current system of obtaining the data from a healthcare provider is sufficient.[11] The medical device manufacturers "believe that patients have the inherent right to access their own medical data[.] [H]owever this in and of itself does not necessitate bypass of any intellectual property protections."[12] However, one patient advocate has asked, "[w]hy is this type of data different from other kinds of digital health data?"[13] In fact, this type of data is even more critically important than other types of digital health information to which patients have ready access. For instance, patients who use continuous positive airway pressure machines (for breathing/snoring) are often unable to access from home the same data as their physician.[14] Patient groups argue that rather than being a mere inconvenience, having to wait to receive data from a physician presents a "massively heightened barrier to vital information whose relevance and importance—such as blood sugar levels or heart rhythms—are often immediate."[15]

This Article aims to begin an important conversation and raise questions that highlight the tension between intellectual property protections and consumer protection. While there are no clear answers, it is important to start thinking about these difficult issues, because so much of modern life involves connected devices sharing data through the "Internet of Things."[16] The legal interests, however, are not clear. While this Article focuses on intellectual property rights and implantable medical devices, many other legal issues are also implicated, including privacy concerns, contractual issues, tort issues, cyber security issues, criminal and constitutional issues, and property

10. *See id.*

11. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. at 65,959.

12. Advanced Medical Technology Association, Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201, at 2 (Mar. 27, 2015), https://www.copyright.gov/1201/2015/comments-032715/class%2027/AdvaMed_Class27_1201_2014.pdf.

13. David Lee Scher, *Data from Implantable Defibrillators and Pacemakers: The World's Best Kept Secret*, DIGITAL HEALTH CORNER (Jan. 30, 2012), https://davidleescher.com/2012/01/30/data-from-implantable-defibrillators-and-pacemakers-the-worlds-best-kept-secret.

14. *See* Amy Dockser Marcus & Christopher Weaver, *Heart Gadgets Test Privacy-Law Limits*, WALL ST. J. (Nov. 28, 2012, 10:31 PM), https://www.wsj.com/articles/SB10001424052970203937004578078820874744076.

15. Public Knowledge, Reply Comments In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. § 1201, at 6 (May 1, 2015), https://www.copyright.gov/1201/2015/reply-comments-050115/class%2027/ReplyComments_LongForm_PublicKnowledge_Class27.pdf.

16. The Internet of Things represents the interconnectedness of objects around us as they communicate data wirelessly to each other. *See* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CAL. L. REV. 805, 812 (2016).

concerns. One interesting aspect further complicating the legal interests in this scenario is that under the current legal paradigm, the patient in whom the device is implanted may not be viewed as the "user" of the device, but rather it may be the physician who implanted the device.[17] Accordingly, some manufacturers take the position that they are prohibited from sharing the patient's data with anyone other than the physician or hospital—not even the patient.[18]

The issues regarding ownership and access in this context are complex and they represent a quintessential example of technology outpacing the law. Two overarching questions are addressed. First, who owns the device and the data? Second, who has or should have access to the data in the device and to the functionality and operability of the device? The short answers to these questions favor the manufacturers.[19] Normative considerations, however, call for a balancing of the control and ownership of data by manufacturers who need these protections to further incentivize their investments in research and development, against broader public policy concerns about individuals' rights to access data that is generated from their bodies.[20] It is also important to peel back the general technological layers involving both hardware and software, in order to better understand relevant concerns and potential solutions.[21] Incidentally, there are over 250,000 mobile health applications and devices available to consumers in the United States.[22] Most of these, such as Fitbit wristbands, are for wellness purposes.[23] This Article does not address this mobile technology. Rather, it focuses only on implantable medical devices.

The questions addressed here are representative of the broader challenges facing regulation of the Internet of Things.[24] Further questions abound. For instance, should consumers have access to data generated from their cars, their refrigerators, their phones? The issues with implantable medical devices present a compelling slice of that larger picture, one that is deeply personal (not merely involving people's possessions but their own bodies) and as such, is a great case study, and a first, for exposing the tensions

17. *See infra* Section II.A.

18. *See infra* Section II.A.

19. *See infra* Section II.C.

20. See Frank Pasquale, *Grand Bargains for Big Data: The Emerging Law of Health Information*, 72 MD. L. REV. 682, 746–47 (2013).

21. *See infra* Section II.B.

22. RESEARCH2GUIDANCE, MHEALTH APP DEVELOPER ECONOMICS 2016: THE CURRENT STATUS AND TRENDS OF THE MHEALTH APP MARKET 12 (2016), https://research2guidance.com/r2g/r2g-mHealth-App-Developer-Economics-2016.pdf.

23. *See Things Are Looking App*, ECONOMIST (Mar. 10, 2016), https://www.economist.com/news/business/21694523-mobile-health-apps-are-becoming-more-capable-and-potentially-rather-useful-things-are-looking.

24. *See generally, e.g.*, Ferguson, *supra* note 16 (discussing the relationship between "smart objects" and the effects clause of the Fourth Amendment).

and interests at stake. "Implants are the most personal among personal chattel. When they become an integral part of our organic body, they also become an intimate part of our identity."[25] Accordingly, to the extent intellectual property rights sometimes need to accommodate weighty public policy concerns, perhaps the unique circumstances presented by patients with implantable medical devices in life or death situations might be a good test case for wrestling with the issues.[26] Ultimately, after exploring the concerns and interests of the stakeholders in this debate, this Article recommends a more nuanced and balanced approach to the sharing of data, as well as consideration of business and technological solutions to supplement and/or complement a legal solution. This framework for thinking about how to balance access rights might also be useful more generally as we continue to face similar questions related to the Internet of Things.

Part II provides background on the key stakeholders in this debate (manufacturers and patients) and how the operation of implantable medical devices raises questions about ownership and access, particularly with the data generated from the devices. Part III explores the relevant areas of intellectual property law (patents, trade secrets, and copyrights) that bear on this issue, as well as other areas of law such as privacy and contracts that are also implicated. A brief review of the regulatory landscape follows in Part IV, including discussion of the Food and Drug Administration's ("FDA") position that manufacturers "may" share patient specific information with patients, as well as the general inapplicability of the Health Insurance Portability and Accountability Act ("HIPAA") to this issue. Furthermore, the regulatory framework that tends to focus mostly on hardware (rather than the software most applicable in this context) may not sufficiently address patient safety and the risks involving software, thus highlighting the interests of independent researchers in these implantable devices.[27]

In Part V, the Article wrestles with the best approaches to move forward, including an exploration of the interests of manufacturers, patients, and researchers. While recognizing that manufacturers must be able to protect their intellectual property rights and their investments in research and development, this Part recommends consideration of data sharing along a more nuanced disclosure spectrum. Thus, this approach asks whether such considerations as the nature of the data requested, the type of device, the context, and the expertise of the recipient might be useful for determining how and what data to share. Moreover, in light of the complex and rigid legal

25. Coalition of Medical Device Researchers, Long Comment Regarding a Proposed Exemption Under 17 U.S.C. § 1201 app. C, at 4 (Feb. 6, 2015), https://copyright.gov/1201/2015/comments-020615/InitialComments_longform_Coalition_of_Medical_Device_Researchers_Class27.pdf.

26. *See* Pasquale, *supra* note 20, at 687 ("Health professionals and patients believe the medical field deserves some autonomy from the normal laws of IP.").

27. *See infra* Section V.A.3.

landscape, business and technical solutions, such as manufacturer-sanctioned mobile health applications that work in conjunction with the implantable devices, might also be considered as a means to providing real-time access to interested patients, as well as possible safe harbors for physicians and manufacturers, to mitigate liability concerns for data sharing. Finally, it is noteworthy that American courts, policymakers, and industries have the opportunity to be at the forefront of this significant and timely issue as other countries, including Europe, also begin to wrestle with related policy concerns.

II. BACKGROUND ON THE STAKEHOLDERS AND DEVICES

For a typical patient, implanted medical devices are implanted by a physician, the hospital bills for the device, and it is paid for by the patient's insurance company.[28] While the interests of medical providers, medical facilities, and insurers are intertwined in these transactions, for the purpose of this discussion of ownership rights and access, the tension lies between manufacturers and patients.

A. THE STAKEHOLDERS

The major stakeholders in issues surrounding implanted medical devices are the manufacturers, vendors, and end users of the devices, who may or may not be the patients themselves. Manufacturers of medical devices are often responsible for all aspects of designing, developing, testing, and manufacturing the implantable device.[29] Implantable medical devices are not sold on the consumer market, but vendors make them available to end-users, who generally are medical facilities.[30] These vendors might provide training and even maintenance of the devices.[31] The users of the medical devices are healthcare professionals, and the patient, into whom the device is implanted.[32] As implanted devices are generally very complex, there typically must be extensive training regarding their operating procedures.[33] Without such training, the level of risk for safety and effectiveness is high.[34]

An interesting irony which further complicates the legal picture is that the patient into whom the device is implanted may not be the "user" of the device. That is because the current legal landscape involving implantable medical devices may all be based on a paradigm reflecting the traditional legal notion that in situations involving a medical device, it is actually the physician

28. Coalition of Medical Device Researchers, *supra* note 25, app. C, at 4.

29. *See* James Williams & Jens Weber-Jahnke, *Regulation of Patient Management Software*, 18 HEALTH L.J. 73, 85 (2010).

30. *Id.*

31. *Id.*

32. *Id.*

33. *Id.*

34. *Id.*

who is considered the user.[35] Indeed, under the learned intermediary doctrine of products liability law, a manufacturer's duty to warn is not to the patient directly, but to the physician as a learned intermediary.[36] This reflects the notion that the physician is in a better position to communicate the information to the patient.[37] Patients technically do not even select their devices; the decision is made for them by the physician and sometimes even by the contracts in place with the medical facility.[38] With the view that it is not the patient, but the physician or hospital that is the customer of the medical device manufacturer, some manufacturers have taken the position that they are prohibited from sharing the patient's data with anyone other than the physician or the hospital—not even the patient.[39] As such, they would require regulatory approval in order to provide patients with their data.[40]

B. THE DEVICES

Modern medical devices are not just equipment; they can be embedded with computer processors and other sophisticated electronics.[41] For instance, implantable defibrillators, glucose monitors, and drug pumps are now relatively commonplace.[42] Other examples of implantable medical devices include spinal cord stimulators and deep brain stimulators.[43]

Among the more common implantable devices are those that treat heart conditions. Pacemakers control abnormal heart rhythms when they are either too slow or too fast. Implantable cardiac pacemakers help to replace or supplement how a defective heart paces itself by delivering electrical pacing pulses to the heart.[44] Implanted defibrillators work by shocking the heart if it senses dangerous rhythms through treatment called defibrillation.[45] Implantable defibrillators deliver electrical energy to the heart in order to reverse excessively rapid heart rates such as life-threatening conditions causing cardiac arrhythmias.[46]

---

35. *See, e.g.*, Rosci v. Acromed, Inc., 669 A.2d 959, 969 (Pa. Super. Ct. 1995).

36. *See, e.g.*, Taylor v. Intuitive Surgical, Inc., 389 P.3d 517, 524 (Wash. 2017).

37. *Id.*

38. *See* Annemarie Bridy, *Trade Secret Prices and High-Tech Devices: How Medical Device Manufacturers Are Seeking to Sustain Profits by Propertizing Prices*, 17 TEX. INTELL. PROP. L.J. 187, 211–13 (2009).

39. *See* Marcus & Weaver, *supra* note 14.

40. *Id.*

41. Williams & Weber-Jahnke, *supra* note 29, at 83.

42. *Id.*

43. *See* LifeScience Alley, Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201, at 4 (Mar. 27, 2015), https://www.copyright.gov/1201/2015/comments-032715/class%2027/LifeScience_Alley_Class27_1201_2014.pdf.

44. Data Logging Sys. for Implantable Med. Device, U.S. Patent No. 6,628,985 (filed Dec. 18, 2000) (issued Sept. 30, 2003).

45. *Pacemakers and Implantable Defibrillators*, MEDLINEPLUS, https://medlineplus.gov/pacemakersandimplantabledefibrillators.html (last updated Jul. 25, 2018).

46. *Id.*

Implantable defibrillators monitor heart rhythm as well as the functional status of the device itself.[47] If, for instance, an arrhythmia is detected, it might signal, even if the patient does not know it's happening.[48] Data collected from the defibrillator is recorded in its memory, and then it is later transmitted to the manufacturer's base station.[49] The data is then sent on to the manufacturer, where it is evaluated and analyzed.[50] The manufacturer will then generate a report that will be available for a fee to the medical provider who may then share it with the patient during his or her appointment.[51] As one patient with a defibrillator describes:

> I am a cyborg of sorts. My every heartbeat is monitored by a built-in computer running proprietary software. But the data it records via sensors in my heart is beyond my reach. It is wirelessly transmitted to a bedside monitor and sent via telephone lines to a monitoring company, bypassing me altogether. I am a cardiac patient living with an implantable cardioverter-defibrillator (ICD).[52]

There is a significant amount of data contained in implantable defibrillators and pacemakers about the patient's heart, and this data is obtained from the device either remotely or during an office visit.[53] However, the devices have limitations. For instance, a defibrillator will not report what exactly a person was doing when he had an arrhythmia, or whether or not he took medication.[54] Thus, the device, no matter how powerful, is merely one tool in the overall treatment of the patient.

The devices also have networking interfaces so that they can interconnect and send data back and forth. The data they collect is usually obtained from the device through what is called interrogation.[55] As such, implantable devices are also producers of data. It is probably also not too far off in the future that there will be autonomous medical devices that share data amongst each other to monitor and treat a patient without intervention from a human.[56] One example of such a device is the hemorrhagic-shock autonomous integrated device ("hemoAID"), created to combat hemorrhagic shock. Hemorrhagic

47. Scher, *supra* note 13.
48. *Id.*
49. Coalition of Medical Device Researchers, *supra* note 25, app. C, at 2.
50. *Id.*
51. *Id.*
52. *Id.* app. C, at 1.
53. Scher, *supra* note 13.
54. *See id.*
55. *See* Method & Apparatus for Enabling Data Commc'n Between an Implantable Med. Device & a Patient Mgmt. Sys., U.S. Patent No. 7,127,300 (filed Dec. 23, 2002) (issued Oct. 24, 2006).
56. *See* Williams & Weber-Jahnke, *supra* note 29, at 83–84.

shock has been associated with changes in plasma vasopressin levels.[57] This device is hoping to neutralize these changes by monitoring vasopressin levels in the plasma and releasing vasopressin automatically when levels are below a certain threshold.[58]

Special equipment known as interrogators are built by the manufacturers and provided to the medical facilities to perform the interrogation function.[59] With a defibrillator, for instance, when it is interrogated, it generates a file containing the patient's data. That file may be stored in a proprietary format that can only be read by the manufacturer's specified program.[60] For devices that are not encrypted, third parties have been able to create their own interrogators.[61] It allows them to obtain information from the patient's device. This facilitates passive interception and transmittal of data from the patient's device on a daily basis, rather than having to wait weeks or months for a doctor's appointment.[62]

For the purposes of this Article, it is not necessary to have an intricate understanding of each device and how it functions beyond what has been described above. In order to arrive at a reasoned approach to balancing the rights of the various stakeholders, it is important to peel back the general technological layers that are implicated in implantable medical devices to better understand the parties' concerns and potential solutions. Put simply then, there is the device in the patient (the hardware), the software that runs the device in the patient, patient data going into the device, data outputs from the device, other hardware that communicate with the implanted device, and software that allows the interconnected hardware to function and communicate. The data outputs from implantable devices can be either in the form of batch reports, or they can be transmitted in real time from the implantable device to the manufacturers' network or other monitoring device.[63] There are also device programmers that transfer information from the implanted device to the manufacturers systems, and information can then be transferred to the medical provider.[64] In addition, data encryption may be used to protect the underlying software. Passwords may be utilized along with encryption to protect patient data, as well as the manufacturer's intellectual property rights.[65]

---

57. Vlad Oncescu et al., *Autonomous Device for Application in Late-Phase Hemorrhagic Shock Prevention*, 9 PLOS ONE e89903, Feb. 2014, at 1, http://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0089903&type=printable.

58. *Id.*

59. *See* U.S. COPYRIGHT OFFICE, *supra* note 7, at 47–48.

60. *See* Coalition of Medical Device Researchers, *supra* note 25, at 7–8.

61. *See* U.S. COPYRIGHT OFFICE, *supra* note 7, at 53.

62. *Id.*

63. Coalition of Medical Device Researchers, *supra* note 25, at 4.

64. *See* Advanced Medical Technology Association, *supra* note 12, at 4.

65. *Id.* at 5.

C. OWNERSHIP & ACCESS QUESTIONS

With a basic understanding of the hardware and software-related components in implantable medical devices, an introduction of the fundamental ownership and access questions are now in order. First, does the patient own the device itself? Perhaps; but not necessarily. The device itself could be owned by the patient as "chattel ownership."[66] The patient usually pays for it as part of a course of treatment. However, this may not necessarily be full ownership, if subject to a lease or license, with the manufacturer retaining some ownership rights. Thus, contracts to the contrary, assume patients own their medical devices. Does it follow then that they should have full access to them? Should the lawful owner of a device have to wait to obtain permission from the manufacturer of the device in order to obtain data from it?

Second, does the patient own the data in the device? She probably does not. The data is owned by the device manufacturer and/or the producer of the software in cases where they are separate entities.[67] Manufacturers own the intellectual property in the software that runs the device[68] and arguably also the data generated from it.

Third, does the patient have full access to the data? She does not. Reports from the data, not necessarily the data itself, may be provided to the patient's medical facility pursuant to the contract with the manufacturer. The treating physician might also have access to a summary report of the data. One physician has noted that "[i]t is rare for any patient . . . to know that they have a right to the data, and rarer that they ask for it."[69]

Fourth, does the patient have control over what could happen to the data collected from his device? He does not. For one thing, HIPAA does not apply to data collected from implantable medical devices.[70] Ironically, data that may not be accessible to a patient himself might nevertheless be used against him. For instance, it is foreseeable that insurers may try to deny certain claims based on the data, or the data might be used to incriminate an individual or determine liability,[71] despite potential issues with the reliability and accuracy of the information.[72] Finally, does the patient have access to knowing how the

66. U.S. COPYRIGHT OFFICE, *supra* note 7, at 38.

67. *See* KAREN SANDLER ET AL., SOFTWARE FREEDOM L. CTR., KILLED BY CODE: SOFTWARE TRANSPARENCY IN IMPLANTABLE MEDICAL DEVICES 3–4 (July 21, 2010), https://www.softwarefreedom.org/resources/2010/transparent-medical-devices.pdf.

68. *See* U.S. COPYRIGHT OFFICE, *supra* note 7, at 38.

69. Scher, *supra* note 13.

70. *See infra* Section IV.B.

71. *See, e.g.*, Kate Crawford, *When Fitbit Is the Expert Witness*, ATLANTIC (Nov. 19, 2014), https://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936; *see also supra* notes 1–2 and accompanying text (discussing State v. Compton, where the defendant was indicted based on data from his implantable pacemaker).

72. Crawford, *supra* note 71.

device works and whether there have been failures or vulnerabilities? No; he definitely does not.

III. THE ROLE OF INTELLECTUAL PROPERTY

This Part will briefly explain the responses in the preceding Section and the areas of IP that allow manufacturers to claim access and ownership to data and devices that a consumer has implanted inside her body. The mix of intellectual property protections available for medical software is complex. Patent and copyright protection can be used on different parts of a software program. Trade secret protection is also available, and these various kinds of protection can be layered to protect the software running the device.[73]

A. PATENT LAW

When a device or software is covered by a patent, broad rights are attached. The patent owner has the right to prevent others from making, using, or selling it. In conjunction with these rights, licensing agreements also help to control and restrict virtually every aspect of the device, even after it has been sold to a consumer. These rights can prevent research and even experimentation on the device. They can also prevent discussion and analysis of vulnerabilities.

Patent protection for software is firmly established as an eligibility question,[74] meaning that software is considered patentable subject matter. There are, however, questions regarding what is necessary for software to receive such protection, and the patent office has issued guidelines.[75] Patents can cover many aspects of implantable medical devices. For example, there are patents on the following: a way to remotely program implantable medical devices,[76] sensors for generating an electrical output signal in cardiac pacemakers,[77] providing wireless communication between an implantable medical device and a host computer,[78] and transmitting information from an implanted device to an external data logging device.[79]

---

73. *See* Paul A. Mathew, *The Next Wave: Federal Regulatory, Intellectual Property, and Tort Liability Considerations for Medical Device Software*, 2 J. MARSHALL REV. INTELL. PROP. L. 259, 303–04 (2003).

74. *See* Diamond v. Dierh, 450 U.S. 175, 192–93 (1981).

75. *See* Examination Guidelines for Computer-Related Inventions, 61 Fed. Reg. 7478 (Feb. 28, 1996).

76. Method & Apparatus for Remotely Programming Implantable Med. Devices, U.S. Patent No. 7,060,031 (filed Feb. 8, 2002) (issued June 13, 2006).

77. High Output Sensor & Accelerometer for Implantable Med. Device, U.S. Patent No. 6,038,475 (filed Nov. 23, 1998) (issued Mar. 14, 2000).

78. Method & Apparatus for Enabling Data Commc'n Between an Implantable Med. Device and a Patient Mgmt. Sys., U.S. Patent No. 7,127,300 (filed Dec. 23, 2002) (issued Oct. 24, 2006).

79. Data Logging Sys. for Implantable Med. Device, U.S. Patent No. 6,628,985 (filed Dec. 18, 2000) (issued Sept. 30, 2003).

B. TRADE SECRET LAW

Trade secret rights also apply in this area to protect the data that is stored and collected, as well as the codes to access or unlock the data. In fact, these rights are sufficiently strong that trade secret owners may refuse to reveal the protected information, even to government regulators.[80] Trade secret rights cover operability and functionality of the devices, and the source code is often a trade secret.[81] Software and streams of data are also transferred in formats that are kept secret by the manufacturer.[82] Accordingly, it does not matter if the device is inside your body, inside your car, inside your phone, or inside your refrigerator. As it currently stands, the protection remains the same.

Trade secret protection covers the ideas and processes in software programs. Trade secrets can protect the source code of the embedded software in medical devices, and it would require formal reverse engineering to reveal the underlying source code for the data.[83] To protect the trade secrets, manufacturers can also require contracts to protect confidentiality of the information and to prevent reverse engineering.[84] Additional measures used to protect the data or codes include the use of proprietary readers, passwords, and encryption.[85] With trade secrecy, however, others may lawfully attempt to reverse engineer the software, unless prohibited by contract.[86]

A combination of trade secrecy and contract law through licensing agreements can be a powerful tool for controlling proprietary data.[87] Agreements with medical providers and medical institutions can also be used to protect a broad range of proprietary information related to medical devices as trade secrets, including the prices of the devices.[88] Indeed, during the course of conducting this research, the author was unable to obtain access to relevant contracts on implantable devices because of confidentiality and non-disclosure limitations.

C. COPYRIGHT LAW

To a lesser extent, copyright law also offers some protections to programmers, and similarly would restrict the ability to tinker with the device or circumvent any technological measures that protect the codes. Some take

80. *See* Elizabeth A. Rowe, *Striking a Balance: When Should Trade-Secret Law Shield Disclosures to the Government?*, 96 IOWA L. REV. 791, 803 (2011).

81. *See* LifeScience Alley, *supra* note 43, at 5.

82. *Id.*

83. *See* Coalition of Medical Device Researchers, *supra* note 25, at 3.

84. *See* Advanced Medical Technology Association, *supra* note 12, at 7.

85. Coalition of Medical Device Researchers, *supra* note 25, at 7–8.

86. In addition to trade secrecy restrictions, there may also be potential liability under the Computer Fraud and Abuse Act for any unauthorized access or intrusions into manufacturers' computers. 18 U.S.C. § 1039(a)(2) (2012).

87. *See* Pasquale, *supra* note 20, at 682.

88. *See* Bridy, *supra* note 38, at 187–89.

the view that the data outputs from implantable devices are probably not subject to copyright protection.[89] It is unclear whether the data outputs from these devices will be protectable under copyright law (since it would depend on the content and arrangement of this data).[90] Unlike patent and trade secret law, copyright law does not protect ideas, processes, or methods of operation.[91] It is therefore sometimes difficult to determine the boundaries of copyright protection when it comes to software.[92] Large portions of software programs containing material that is either in the public domain or that is not creative expression would not qualify for copyright protection. Reverse engineering of a computer program could be lawful if trying to discover non-protectable portions of the program.[93]

Even though copyright law only protects the expression of an idea, the protection of software is not limited to an exact copy of the source or object code. For instance, the Second Circuit created the "Abstraction-Filtration-Comparison" test, which "determine[s] whether the non-literal elements of two or more computer programs are substantially similar."[94] This test breaks down the program into structural parts, filters out portions that are not protectable in copyright law, such as portions in the public domain or designed for efficiency, and then compares the remaining code.[95] This analysis allows someone to protect the code from any form of copying. Just as one cannot copy a book by substituting each word with a synonym, one cannot copy a program by substituting lines of code with functional equivalents.

The Digital Millennium Copyright Act ("DMCA") was enacted in 1998 to help protect copyrighted works by restricting the ability to circumvent certain access controls such as an encryption.[96] There are exceptions to the DMCA for various types of reverse engineering, encryption, research, and security testing.[97] The Register of Copyrights has noted that the outputs generated by implantable medical devices are not likely to be covered under copyright

89. *See* Public Knowledge, *supra* note 15, at 4.

90. Coalition of Medical Device Researchers, *supra* note 25, at 6.

91. 17 U.S.C. § 102(b).

92. *Compare* Whelan Assocs., Inc, v. Jaslow Dental Lab., Inc., 797 F.2d 1222, 1248 (3d Cir. 1986) (finding that a recordkeeping software program developed by a dental laboratory was substantially similar to a competing program, written in another coding language, and holding that "copyright protection of computer programs may extend beyond the programs' literal code to their structure, sequence, and organization"), *with* Nichols v. Universal Pictures Corp., 45 F.2d 119, 121 (2d Cir. 1930) (holding that, while "two plays may correspond in plot closely enough for infringement," the plot of the defendant's film did not so closely correspond with the plot of the plaintiff's play that his copyright had been infringed).

93. *See* Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1527 (9th Cir. 1992); *infra* Section V.B.

94. Computer Assocs. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 706 (2d Cir. 1992).

95. *Id.*

96. *See* Brenda M. Simon, *Patent Cover-Up*, 47 HOUS. L. REV. 1299, 1325 (2011).

97. *Id.*

law.[98] Some data outputs might qualify for protection only if they reflected a sufficiently original selection and presentation of the data.[99]

Some manufacturers have argued, however, that the outputs for the medical devices would be entitled to copyright protection because of their structure, format, and arrangement, and that any use of that output would not be fair use under copyright law.[100] However, to the extent raw data is transferred from the patient's implantable to a phone or other device or to a new database not copied from the manufacturer's original database, this is not likely to be protected from copyright or might be fair use.[101]

D. INTERSECTION WITH OTHER AREAS OF LAW

Not only do consumers not have access to the data or important decisions concerning the data recorded by many implanted devices, many times they also have no control over how it could be used, whether it could be given to the government, to advertisers, or any other parties. While this Article focuses on intellectual property rights, this topic implicates a host of other legal issues including privacy concerns, contractual issues, tort issues, cyber security issues, criminal and constitutional issues, and property concerns. However, none of those areas, as it currently stands, would either in theory or practice likely resolve the balancing in favor of the patient.

1. Privacy

As compared to the clarity of intellectual property rights, privacy rights for consumers in this context is quite murky and unsettled.[102] A reason for this is that the word "privacy" can have many definitions, depending on context. Three different contexts include privacy in physical space, privacy relating to making choices, and privacy in the sharing of personal information.[103] Moreover, current federal and state protections are not comprehensive, or as efficient in keeping up with technological advances.[104] Health information received its own statutory federal privacy protections with

98. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65,944, 65,959 (Oct. 28, 2015) (codified at 37 C.F.R. § 201.40 (2017)).

99. *Id.*

100. *See* Advanced Medical Technology Association, *supra* note 12, at 4.

101. *See* NAT'L TELECOMM. & INFO. ADMIN., RECOMMENDATIONS OF THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION TO THE REGISTER OF COPYRIGHTS 60–61 (Sept. 18, 2015), https://www.copyright.gov/1201/2015/2015_NTIA_Letter.pdf.

102. *See, e.g.*, Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201, 1232–33 (2000).

103. Jerry Kang, *Information in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202–04 (1998).

104. Patricia I. Carter, *Health Information Privacy: Can Congress Protect Confidential Medical Information in the "Information Age"?*, 25 WM. MITCHELL L. REV. 223, 241 (1999).

the passage of HIPAA.[105] However, not even HIPAA provides specific privacy rights to patients in their information.[106]

There have been some privacy concerns raised when law enforcement has used tools such as GPS tracking and other tools to remotely access information from individuals.[107] In some ways, though, this is a different situation because those individuals are not consenting to the use of the devices in the same way that a patient with an implantable medical device would. Indeed, as noted in the introduction, an Ohio man was indicted on charges of arson and insurance fraud using data from his pacemaker. [108] A cardiologist concluded that his recorded heart rate rhythms were inconsistent with his version of how the fire occurred.[109] This highlights an interesting irony: Information in an implantable device can be used against a patient by the government, but not by the patient themselves in some circumstances. Indeed, it will be interesting to consider the extent to which the Fourth Amendment jurisprudence might contribute (if at all) to a framework for protecting data emanating from one's body and the expectations of privacy resulting therefrom. As it stands now, however, that area is too muddled to offer any assistance.[110]

2. Contracts

General principles of contract law require mutual assent to form a contract.[111] Sometimes, however, particularly in situations where a patient signs a contract with a medical provider without the ability to negotiate its terms, it is referred to as a contract of adhesion. These contracts are not necessarily invalid, but courts may examine the terms more closely to

105. *See infra* Section IV.B.

106. *See* Zittrain, *supra* note 102, at 1237; s*ee also infra* Section IV.B (discussing the application of HIPPA to medical device data).

107. *See, e.g.*, Ferguson, *supra* note 16, at 830–32 (discussing the right of privacy in the context of law enforcement use of GPS devices); Joel Kurth & Lauren Abdel-Razzaq, *Device Lets Oakland Deputies Track Cellphones*, DETROIT NEWS (April 7, 2014), EBSCOHOST NEWSPAPER SOURCE PLUS, accession no. AP2f786558o0b864ec9aae10cfa4bce01ec (last visited Aug. 3, 2018) (discussing the "Hailstorm" device that law enforcement uses to gather cellphone data); Abby Simmons, *Dec. 27, 2013: Minnesota Legislators Challenge Police Collection of Phone Data*, STAR TRIBUNE (Sept. 19, 2014, 7:56 PM), http://www.startribune.com/dec-27-2013-minnesota-lawmakers-question-police-use-of-snooping-devices/237405981 (reporting on the Minnesota legislature's efforts to investigate police use of devices that collect cellphone data).

108. *See* Matyszczyk, *supra* note 2.

109. *Id.*

110. *See, e.g.*, United States v. Jones, 565 U.S. 400, 413–15 (2012) (Sotomayor, J., concurring) (arguing that in addition to Justice Scalia's trespass view of the Fourth Amendment, the Court could find a violation of the Fourth Amendment based on a reasonable expectation of privacy); Ferguson, *supra* note 16, at 829 ("Scholars who study the Fourth Amendment agree that new technologies have created some fascinating and largely unanswered doctrinal puzzles.").

111. 1 WILLISTON ON CONTRACTS § 4:1 (4th ed. 2018).

determine whether they are unconscionable.[112] Naturally, these agreements will often be more favorable to the party that drafted them, rather than the patient or consumer.[113] Nevertheless, it is possible to envision contract law as a means to further support greater sharing in this context, while respecting the rights of manufacturers.[114]

Written agreements between the medical device manufacturers and the physicians and hospitals may also contain terms restricting how the data may be shared and by whom.[115] Thus, the hospital or physician may be the only ones contractually permitted to disclose the patient's data to the patient (and even then perhaps only the summary reports and not the raw data itself).

There are likely to be several contracts involved with the healthcare facility for each implantable medical device. For instance, there may be separate licenses for the software, the equipment, ongoing maintenance of the software and the equipment, and perhaps contracts regulating the data itself.[116] These contracts may also contain nondisclosure agreements, preventing, among other things, disclosure of any software related incidents or defects.

IV. REGULATORY OVERSIGHT

There is also significant regulatory fragmentation between and among the various government agencies that might each independently have some oversight over implantable medical devices. Several government agencies potentially have a hand in this regulatory space, including, for instance, the Copyright Office, the FCC, the FTC, the Department of Health and Human Services, the FDA, and the Department of Homeland Security. This Part briefly discusses their respective roles.

A. FDA

The Food and Drug Administration ("FDA") has the power to regulate the use of medical devices under the Federal Food, Drug, and Cosmetic Act.[117] Some medical device manufacturers have taken the position that they would require regulatory approval in order to provide patients with their data.[118] In 2016, FDA's Center for Devices and Radiological Health produced

112. *See* Jay P. Kesan et al., *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 424 (2013).

113. *Id.*

114. *See* Andrea M. Matwyshyn, *Privacy, The Hacker Way*, 87 S. CAL. L. REV. 1, 5 (2013) (arguing that contract law can be used as a means to protect consumer privacy).

115. *See* Marcus & Weaver, *supra* note 14.

116. *See, e.g.*, Lisa L. Dahm, *Restatement (Second) Of Torts Section 324A: An Innovative Theory of Recovery for Patients Injured Through Use Or Misuse Of Health Care Information Systems*, 14 J. MARSHALL J. COMPUTER & INFO. L. 73, 105 n.158 (1995).

117. Federal Food, Drug, and Cosmetic Act § 201(h), 21 U.S.C. § 321(h) (2012).

118. *See* Marcus & Weaver, *supra* note 14.

draft guidance on "Dissemination Of Patient-Specific Information From Devices by Device Manufacturers."[119] This draft guidance provides that manufacturers "may share patient-specific information" from a medical device with the patient who is being treated with the device.[120] This language does not require sharing, nor does it prescribe how the sharing might occur.

The 21st Century Cures Act[121] is an example of recent legislation that some argue lowers the standards necessary for FDA to approve medical devices. The Act permits, among other things, approval of medical devices in some situations without requiring clinical trials.[122] This might therefore be even more of a reason to encourage independent research on medical devices, since patients may potentially be made more vulnerable from the reduction of premarket testing. The Act also modified its definition of a device to make clear that standalone software will not be regulated by FDA as a device.[123] This seems to mostly apply to software that is intended to run on general-purpose computers and that does not diagnose or treat conditions. The 21st Century Cures Act includes the type of software that was already considered "medical device data systems," that basically collect information rather than analyze or interpret patient information with the purpose of diagnosing, curing, mitigating, preventing, or treating a condition or disease.[124] Thus, it is more applicable to mobile health apps than to implanted devices. Arguably, the kinds of software embedded in implanted devices that is used for the purpose of making clinical decisions is covered separately under FDA's Draft Guidance on "Software As a Medical Device."[125]

119. Dissemination of Patient-Specific Information From Devices by Device Manufacturers; Draft Guidance for Industry and Food and Drug Administration Staff; Availability, 81 Fed. Reg. 37,603 (June 10, 2016).

120. CTR. FOR DEVICES & RADIOLOGICAL HEALTH, FOOD & DRUG ADMIN., MANUFACTURERS SHARING PATIENT-SPECIFIC INFORMATION FROM MEDICAL DEVICES WITH PATIENTS UPON REQUEST: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 2 (2017), https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm505756.pdf.

121. 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (2016).

122. *See* Trudy Lieberman, *21st Century Cures Act: A Huge Step Backward for FDA Standards*, HEALTHNEWSREVIEW.ORG (Aug. 4, 2015), https://www.healthnewsreview.org/2015/08/21st-century-cures-act-a-huge-step-backward-for-fda-standards.

123. 21st Century Cures Act § 3060, 21 U.S.C. § 360j(o) (2012 & Supp. V 2017).

124. Medical Device Data System, 21 C.F.R. § 880.6310 (2018).

125. CTR. FOR DEVICES & RADIOLOGICAL HEALTH, FOOD & DRUG ADMIN., SOFTWARE AS A MEDICAL DEVICE (SAMD): CLINICAL EVALUATION: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 10 (2017), https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm524904.pdf.

B. HIPAA

The privacy of medical and health information is protected under the Health Insurance Portability and Accountability Act ("HIPAA").[126] Pursuant to HIPAA, the Department of Health and Human Services has enacted regulations regarding the collection, security, distribution, and use of personal healthcare information subject to HIPAA.[127] One such regulation is the HIPAA Privacy Rule. The Rule is intended to regulate the disclosure of identifiable health information.[128] Among other things, it requires healthcare providers to keep data confidential and also regulates the sharing of patient records.[129] Separately, the HIPAA Security Rule governs the security of health care data that is stored.[130] The bottom line, though, is that HIPAA regulates medical records and "protected health information,"[131] neither of which encompasses the kinds of data generated from implantable medical devices.

Put simply, HIPAA generally regulates the sharing of patient information with third parties. The issue in the context of implantable medical devices, however, is about the patient receiving his or her own information. In general, neither HIPAA nor any other law prevents patients from accessing their own medical records or disclosing their own information to others directly.[132] Probably the most applicable and helpful provision of HIPAA in this context is its requirement that individuals have a right to access their health information.[133] It may be that the availability of the information from the physician's office or hospital is sufficient to meet this requirement. However, this begs an important question: What is the extent of an individual's right to access one's own information?

HIPAA applies to "protected health information"[134] or "individually identifiable health information" when it is collected by such entities as health plans, healthcare providers, or employers.[135] HIPAA also contains standards to govern storage, maintenance, and transmission of personal health

126. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

127. *See* 45 C.F.R. §§ 160.101–164.534 (2017).

128. *Id.* § 164.502(a).

129. *Id.* §§ 160.101–164.534.

130. *Id.* § 164.306(a).

131. *Id.* § 160.103.

132. *See* Public Knowledge, *supra* note 15, at 8–9.

133. *See* 45 C.F.R. § 164.524(a)(1).

134. *Id.* § 160.103 (defining protected health information as "[i]ndividually identifiable health information, including demographic information collected from an individual" that "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to the individual; or the past, present, or future payment for the provision of healthcare to the individual; and . . . [t]hat identifies the individual; or . . . [w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual.").

135. *Id.* §§ 160.103, 164.502.

information.[136] In addition, it imposes privacy requirements for the information that it covers. However, the specific privacy and security safeguards under HIPAA do not apply to medical device data.[137] Accordingly, some manufacturers take the position that they own the data collected by the devices they manufacture, not the patient or the medical provider.[138] Therefore, when a patient wears a heart monitor, the contractual terms provide that the manufacturer owns the data collected from the patient.[139] Relatedly, HIPAA's coverage also falls short in another area where patients may assume they have protection. Because HIPAA only protects identifiable information, patients' medical information from labs, pharmacies, and physicians can be traded and sold as long as their names are removed, and even without the patients' knowledge or consent.[140]

Separately from the data or information, medical device manufacturers as a group are not necessarily subject to HIPAA in this context. Ultimately, the analysis would depend on whether the manufacturer is considered a "covered entity"[141] and if so, whether the data generated by the medical device is "protected health information" under HIPAA. Whether, pursuant to the Privacy Rules, the manufacturer is deemed to provide "healthcare" to a patient would also be relevant.[142] Typically, if a company is merely selling its products to a facility for that entity to use with patients, it is not providing "healthcare."[143]

The HIPAA Privacy Rule and Security Rule are only applicable to medical device manufacturers if they are considered a "covered entity" or "business associate" per the terms of the regulation.[144] Generally, covered entities are, healthcare providers and health plans that electronically transmit patients'

136. *Id.* §§ 164.310–.314.

137. *See* GEORGE B. DELTA & JEFFREY H. MATSUURA, LAW OF THE INTERNET § 3.03 (4th ed. 2016 & Supp. 2018).

138. *See* Marchs & Weaver, *supra* note 14.

139. *See id.*

140. *See* ADAM TANNER, OUR BODIES OUR DATA: HOW COMPANIES MAKE BILLIONS SELLING OUR MEDICAL RECORDS 147 (2017).

141. Some medical device companies may be considered "covered entities" if they sell directly to patients and bill Medicare. *See, e.g.*, Robert Klepinski, *Privacy Basics: A Quick HIPAA Check for Medical Device Companies*, MED. DEVICE & DIAGNOSTIC INDUS. (Aug. 1, 2009), http://www.mddionline.com/article/privacy-basics-quick-hipaa-check-medical-device-companies.

142. *See* Louiza Dudin, *Networked Medical Devices: Finding a Legislative Solution to Guide Healthcare Into the Future*, 40 SEATTLE U. L. REV. 1085, 1093–94 (2017).

143. *See When May a Covered Health Care Provider Disclose Protected Health Information, Without an Authorization or Business Associate Agreement, to a Medical Device Company Representative*, U.S. DEP'T OF HEALTH & HUMAN SERVS., (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/faq/490/when-may-a-covered-health-care-provider-disclose-protected-health-information-without-authorization/index.html.

144. *See* J. Mason Weeda, *FDA Publishes Draft Guidance on Dissemination of Patient-Specific Data —But Doesn't Say Much About HIPAA*, OFW LAW (June 15, 2016), http://www.ofwlaw.com/2016/06/15/fda-publishes-draft-guidance-dissemination-patient-specific-data-doesnt-say-much-hipaa.

"protected health information."[145] Medical device manufacturers could be considered covered entities or business associates under limited circumstances, such as when a manufacturer's representative is present in an operating room to provide guidance on use of its device on a patient.[146] However, in the circumstances related to the kinds of situations involving implantable medical devices discussed in this Article, the same is not likely to be true.[147] Furthermore, because the raw data gathered by an implant is not technically being held by a physician or hospital,[148] it may not be covered by HIPAA. Instead, it goes directly to the device manufacturer who then provides a summary report to the physician.[149]

Interestingly, the draft guidance issued by the FDA[150] which suggests that manufacturers share information with patients from their medical devices, does not specifically address HIPAA. Nor does it discuss whether device manufacturers are subject to HIPAA requirements.[151] The FDA Guidance applies to "patient-specific information" which is clinical data such as heart electrical activity, rhythms monitored by a pacemaker, and pulse oximetry data.[152] Therefore, given that HIPAA protects patient information that is individually identifiable, it is questionable whether any of this data would be covered by HIPAA, unless the patient is somehow identifiable.[153]

HIPAA, as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH")[154] addresses the privacy and security of electronic transmission of protected health information.[155] It also strengthens the civil and criminal enforcement of the HIPAA rules.[156] It contains a provision that patients should be provided with electronic copies of their health information upon request, including diagnostic test results.[157] In particular, it provides that an "individual shall have a right to obtain from such covered entity a copy of such information in electronic format and, if

145. *Id.*

146. *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 143; Weeda, *supra* note 144.

147. Even if HIPAA were applicable in these circumstances, it is unlikely that patient authorization would be required, given the exceptions to the Privacy Rule that would allow patients' data to be used and disclosed without authorization since it is being used for the patient's treatment. *See* 45 C.F.R. § 164.506(c) (2017).

148. *See* Marcus & Weaver, *supra* note 14.

149. *Id.*

150. *See generally* CTR. FOR DEVICES & RADIOLOGICAL HEALTH, *supra* note 120 (providing nonbinding guidance to device manufacturers on sharing "patient-specific information" at the patient's request).

151. *See* Weeda, *supra* note 144.

152. CTR. FOR DEVICES & RADIOLOGICAL HEALTH, *supra* note 120, at 2.

153. *See* Weeda, *supra* note 144.

154. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified as amended in scattered sections of 42 U.S.C.).

155. 42 U.S.C. § 17932 (2012).

156. *Id.* § 17931(b).

157. *Id.* § 17935(e)(1).

the individual chooses, to direct the covered entity to transmit such copy directly to an entity or person designated by the individual."[158] It applies to a covered entity (under HIPAA) that maintains, retains, modifies, or accesses information from a medical device.[159] One could argue that the kinds of data provided from implantable devices (such as the rhythm from an implantable defibrillator) is captured by this requirement, but it would not necessarily require the provision of real-time access to the data.[160] Thus, a gap remains when it comes to patients' access to data from implanted medical devices. Put simply, HIPAA and HITECH grant patients access to their "traditional" medical records that are maintained by a health provider or covered entity. In the case of data generated from the patient, however, the definitions in coverage (as described above) fall short or are, at best, ambiguous. Thus, questions remain. Is the data "protected health information" that would be the kind of medical record envisioned under the Act? Even if it were, is the device manufacturer (or whoever collects the data) a "covered entity" or "provider"? Finally, even if it were, nothing in the Act seems to suggest that access to the data in real time would be required.

C. FTC & FCC

The Federal Trade Commission ("FTC") has been promoting its initiatives with respect to consumer protection laws and privacy for mobile applications—but not so much for medical devices. The Federal Trade Commission Act empowers the FTC to prevent the use of "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[161] Therefore, the agency's authority tends to be limited to enforcement of conduct when companies are engaging in deceptive or unfair practices.[162] Arguably, the FTC, from a consumer protection perspective, could require that consumers receive their data, but the agency has not yet weighed in on this issue.

The Federal Communications Commission ("FCC") generally has authority to regulate the radio frequencies used in the transmission of data. It therefore shares jurisdiction over wireless devices, which might include implantable devices, like pacemakers. It has jurisdiction over the electromagnetic spectrum used to transmit information wirelessly from

158. *Id.*

159. *See id.*

160. *See* David Lee Scher, *Five Reasons Why Patients with Implantable Defibrillators Deserve Their Data*, DIGITAL HEALTH CORNER (Jan. 26, 2012), https://davidleescher.com/2012/01/26/five-reasons-why-patients-with-implantable-defibrillators-deserve-their-data.

161. 15 U.S.C. § 45(a)(2).

162. *See id.*

medical devices.[163] Similar to the FTC, there might be potential for some level of intervention, but no such indications have appeared.

V. MOVING FORWARD

Ultimately, it is important to determine how to achieve the appropriate balance among all the various constituents and their respective interests in this puzzle. Decision makers would be remiss to overlook patients/consumers, because innovation (which typically is given as a purpose for strong intellectual property rights) might also be dependent on consumers and not just stronger intellectual property protections. This is because if consumers cannot trust implantable devices, then what happens to the market? The challenge is trying to weigh what should be done as a matter of intellectual property policy while also being mindful of health policy and patients' rights.

A. PARTIES' INTERESTS

One patient articulates the problem as follows: "Implanted devices should answer first to us, then to our doctor, and finally, maybe, to a manufacturer. Right now that sequence is reversed."[164] Is he correct or is the answer more nuanced? In this Part, the Article highlights the various key interests at stake, particularly those of manufacturers, patients, and researchers.

1. Manufacturers

Manufacturers ought to be able to protect their intellectual property rights. Nothing in this Article should be read to suggest otherwise, because it is important to preserve expenditures in research and development and to spur further innovation that ultimately benefits consumers. Manufacturers expend tremendous amounts of resources in research and development in order to build and create these life-saving devices. For instance, as a result of decades of investment in research, development, and innovation, the pacemaker has evolved from the size of a toaster oven to the size of a quarter, while retaining tremendous processing power from its embedded software.[165] This is the kind of innovation that no doubt benefits all the stakeholders.

Medical device manufacturers have argued that they "believe that patients have the inherent right to access their own medical data[.] [H]owever this in and of itself does not necessitate bypass of any intellectual property protections."[166] They argue that if patients were to directly access

163. *See* Brian Dolan & Russell Fox, *Understanding mHealth regulation: FCC and FDA*, MOBIHEALTHNEWS (June 26, 2009), http://www.mobihealthnews.com/2960/understanding-mhealth-regulation-fcc-and-fda.

164. Coalition of Medical Device Researchers, *supra* note 25, app. C, at 4.

165. *See* Bridy, *supra* note 38, at 209.

166. *See* Advanced Medical Technology Association, *supra* note 12, at 2.

their data on their devices, they may have difficulty understanding and interpreting the data, since they lack the appropriate tools and training that are provided to a medical professional.[167] It should also be noted that many patients may not wish to have real-time or detailed access to the data from their devices.

Manufacturers' desire to protect their intellectual property rights in implantable medical devices is reasonable and it is imperative that they do so. From the manufacturers' perspective, documents and data related to implantable medical devices should be treated as if they are trade secrets. This means ensuring physical safeguards for all paper and electronic documents and databases through such protective methods as encryption and passwords. Trade secret data must be segregated from other kinds of data, particularly when they are made available to third parties, and all such parties should execute confidentiality agreements. Furthermore, the information should only be shared on a need to know basis.

Where applicable, copyright protection should also be sought for the software. This would provide an additional measure of protection for some of the content that may be deemed sufficiently expressive and creative. Patent protection can also be extremely valuable, even though it is much more expensive. This would especially provide protections against reverse engineering. Contracts also continue to be vital to buttressing all these intellectual property protections, as the specific agreements between the parties can sometimes provide extra protection beyond that which is available in each individual area of intellectual property.

2. Patients

Patients argue that they may be harmed by the inability to react to data collected by their medical devices in real time because, for instance, they may not be able to detect drops in their heart rate or spikes in their glucose. Instead, they must wait for a medical appointment in order to obtain this information. As one commentator has noted: "[I]f a patient receives a report at the doctor's office showing a glucose spike three weeks ago at a certain time, the patient will likely not remember what happened at that moment, and will be unable to take remedial action in order to prevent that kind of spike from repeating."[168]

To better understand this concern, it might be helpful to understand how a continuous glucose monitor works. There is a small sensor inserted under the skin which is replaced every seven days and there is also a handheld receiving computer which shows the current glucose value.[169] "The sensor transmits a new sensor value every five minutes" in the handheld receiving

167. *Id.*

168. NAT'L TELECOMM. & INFO. ADMIN., *supra* note 101, at 60.

169. U.S. COPYRIGHT OFFICE, *supra* note 7, at 8.

computer, and "shows the last value [along] with an overall trend."[170] Patients, however, may wish to have additional information beyond what is on their display, such as the difference between the current glucose number and the previous one, or they may wish to have the information transferred to their mobile phone.[171] This may help them decide whether they need to act immediately to ingest sugar if the insulin level is too high.[172] While some of the glucose monitors on the market have been unencrypted, the newest ones will be protected with encryption, making it more difficult for patients to reverse engineer this information in order to learn how the machines work.[173]

Some of the arguments that have been made on behalf of patients' right to access their data include increased patient engagement, better understanding about how the devices work, better understanding of the need for medication, and better communication between patients and their other medical providers. Thus, a patient suffering from heart disease, for instance, should be able to share information with his primary care provider to better coordinate his healthcare.[174]

Patients can also improve their treatment outcomes by actively monitoring their own information.[175] Because patients are unable to access the real-time data about what is happening in their bodies, some argue that they may not be able to detect potential errors from the implantable devices, or worse yet, they cannot determine when a medical emergency might be occurring.[176] As one patient has noted, "[a]s helpful as it is to doctors, I believe access to information stored in the [defibrillator] is mostly beneficial to patients who live with the condition, not to doctors who care for them."[177] For instance, knowing that a change in chest impedance could signal excessive water retention, may allow a patient to take faster corrective action.[178]

3. Safety, Cybersecurity & Research

The current regulatory framework that tends to focus mostly on hardware may not sufficiently address patient safety. Given the evolution from equipment/hardware to the introduction of embedded software, it is noteworthy that even traditional language about devices such as requirements for sterilization and protection against flammability, do not specifically refer

170. *Id.*
171. *Id.* at 9.
172. *Id.* at 10.
173. *Id.* at 58–60.
174. *See* Scher, *supra* note 13.
175. *See* Coalition of Medical Device Researchers, *supra* note 25, at 18–19.
176. *See id.* at 5, 18–19.
177. *Id.* app. C, at 2.
178. *Id.* app. C, at 2–3.

to software.[179] The properties of software are very different from mere mechanical devices, regulation of which is centered around their physical properties.[180] As such, it is important to be mindful of risks involving software.

Devices do malfunction and can be flawed. Some, for instance, can be excessively fragile and prone to fracturing. Some may be unreliable, some may provide poor electrical outputs.[181] There have been injuries resulting from design and programming errors in medical devices and software failure has led to device recalls.[182] There can be programming errors, and errors in calibration of the devices that could lead to negative consequences for patients.[183] According to one commentator, software "code inevitably has bugs[,] [and] [i]t is practically impossible if not actually impossible for manufacturers to eliminate all the bugs before devices go on the market."[184]

Many devices on the market are actually not encrypted.[185] Medical device manufacturers do not always encrypt data outputs and computer codes.[186] As a result, the FDA issued new guidance strongly encouraging encryption of medical devices.[187] Ironically, this has created a double-edged problem: Without encryption, patients and researchers are able to tinker with their devices more easily. However, this has also made them more vulnerable to bad actors. This was part of the reason motivating the DMCA exemption discussed below.[188]

There are also cybersecurity concerns, including reports that the Department of Homeland Security is investigating dozens of cyber security flaws in medical devices.[189] Nevertheless, design flaws in software contributing to such errors as software miscommunication and other device malfunctions are an even more real threat than the threat from cybersecurity breaches.[190]

---

179. *See* 21 C.F.R. pt. 880 (2018).

180. *See generally id.* (regulating the properties of "of general hospital and personal use devices intended for human use that are in commercial distribution" including, *inter alia*, hospital bedding and bandages).

181. *See* High Output Sensor & Accelerometer for Implantable Med. Device, U.S. Patent No. 6,038,475 (filed Nov. 23, 1998) (issued Mar. 14, 2000).

182. *See* Coalition of Medical Device Researchers, *supra* note 25, at 2–3.

183. *See, e.g.*, Barry Meier, *Maker of Heart Device Kept Flaw from Doctors*, N.Y. TIMES (May 24, 2005), http://www.nytimes.com/2005/05/24/business/maker-of-heart-device-kept-flaw-from-doctors.html.

184. U.S. COPYRIGHT OFFICE, *supra* note 7, at 41.

185. *See id.* at 15, 41, 53.

186. *See* Coalition of Medical Device Researchers, *supra* note 25, at 3, app. E, at 2.

187. CTR. FOR DEVICES & RADIOLOGICAL HEALTH, FOOD & DRUG ADMIN., CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 5 (2014), https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf.

188. *See* U.S. COPYRIGHT OFFICE, *supra* note 7, at 60–61.

189. Jim Finkle, *U.S. Government Probes Medical Devices for Possible Cyber Flaws*, RECODE (Oct. 22, 2014, 1:39 AM), https://www.recode.net/2014/10/22/11632130/u-s-government-probes-medical-devices-for-possible-cyber-flaws.

190. *See* U.S. COPYRIGHT OFFICE, *supra* note 7, at 25.

Indeed, hundreds of recalls are issued each year for software issues in medical devices.[191]

In other work,[192] I have also raised concerns about the use of intellectual property and licensing to inhibit legitimate research. A similar concern is also present in this area as researchers may not have access to the data or functionality from these medical devices in order to lend any oversight and/or independent research.[193] In order to access the code and outputs from these implantable medical devices, researchers will usually need to intercept the radio transmission and then decode the transmissions using reverse engineering techniques.[194] This could then be used to reveal the underlying source code.[195]

Independent researchers often discover vulnerabilities and flaws in these devices.[196] One such story of note was the discovery of dangerous vulnerabilities with insulin pumps.[197] Accordingly, even the FDA promotes and recognizes the value of independent research.[198] Such research is helpful in guiding and improving FDA regulations.[199] One researcher has noted that "robust security research will help medical professionals and patients make informed choices."[200]

B. CIRCUMVENTION

Recognizing that law alone may not provide the answer to the access problem, technological considerations may add another piece to this puzzle. For instance, some patients have taken matters into their own hands and are prepared to hack into their own devices in order to obtain access. They have also taken to social media.[201]

In 2015, a group of patients and researchers calling themselves the Coalition of Medical Device Researchers filed a petition with the Library of

191. *Id.*

192. *See generally* Elizabeth A. Rowe, *Patents, Genetically Modified Foods, and IP Overreaching*, 64 SMU L. REV. 859 (2011) (discussing the use of license agreements and patent law to inhibit research on genetically modified organisms).

193. *See* Pasquale, *supra* note 20, at 738.

194. Coalition of Medical Device Researchers, *supra* note 25, at 10.

195. *Id.*

196. For a sample bibliography of independent research on medical device safety, see *id.* app. B.

197. Jordan Robertson, *The Trials of a Diabetic Hacker*, BLOOMBERG (Feb. 23, 2012, 4:31 PM), https://www.bloomberg.com/news/articles/2012-02-23/the-trials-of-a-diabetic-hacker.

198. U.S. COPYRIGHT OFFICE, *supra* note 7, at 28–29.

199. *Id.*

200. *Id.* at 57.

201. *See* #wearenotwaiting, TWITTER, https://twitter.com/hashtag/wearenotwaiting (last visited Aug. 4, 2018); CGM in the Cloud, FACEBOOK, https://www.facebook.com/groups/cgminthecloud (last visited Aug. 4, 2018); *The #WeAreNotWaiting Diabetes DIY Movement*, HEALTHLINE, http://www.healthline.com/health/diabetesmine/innovation/we-are-not-waiting (last visited Aug. 4, 2018); *Welcome to Nightscout*, NIGHTSCOUT, http://www.nightscout.info (last visited Aug. 4, 2018).

Congress seeking an exemption to the Digital Millennium Copyright Act ("DMCA") provisions that ordinarily blocks circumvention of technologically protective measures ("TPM") around their implantable devices.[202] Such measures included, for instance, encryption on the outputs of medical devices or home monitoring systems, password systems that control access to patient management software and devices, and proprietary software and tools for extracting device information.[203] The petition sought to allow research into software flaws on these devices as well as to allow patients to access information generated by their own devices.[204] The coalition explained that patients needed real-time access to their own healthcare data in order to help them detect major health risks.[205] Their proposed exemption sought access to TPM-protected data outputs from medical devices only, and not more broadly to the computer programs embedded in the devices, or their monitoring systems.[206]

Not surprisingly, the manufacturers and copyright holders opposed the exemption. They argued that the patient's ability to receive reports from his or her health care provider was sufficient access. They also expressed health and safety concerns from allowing circumventions.[207] Those opposing the exemption also included FDA,[208] the Intellectual Property Owners Association, the National Association of Manufacturers, the Advanced Medical Technology Association, and LifeScience Alley.[209] They argued that circumvention would create incentives to misuse devices and would pose unnecessarily high risks to patients.[210] They further argued that device security research is already ongoing and that research is encouraged with proper agreements with the manufacturers.[211] They also raise concerns that

202. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65,944, 65,955 (codified at 37 C.F.R. § 201.40 (2017)); Coalition of Medical Device Researchers, *supra* note 25, at 1.

203. Coalition of Medical Device Researchers, *supra* note 25, at 7–9.

204. *Id.* at 4–5.

205. *Id.* at 3.

206. *See id.* at 7–9.

207. LifeScience Alley, *supra* note 43, at 4.

208. U.S. Dep't of Health & Human Servs., Food & Drug Admin., Opinion Letter on Section 1201 Rulemaking—Proposed Exemption for Medical Devices (Aug. 18, 2015), https://www.copyright.gov/1201/2015/USCO-letters/FDA_Letter_to_USCO_re_1201.pdf.

209. *2015 Anticircumvention Rulemaking Proceeding*, CYBERLAW CLINIC, http://blogs.harvard.edu/cyberlawclinic/2015-dmca (last visited Aug. 4, 2018).

210. *See* Advanced Medical Technology Association, *supra* note 12, at 4.

211. *See* 510(K) Coalition, Short Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201 (Mar. 27, 2015), https://www.copyright.gov/1201/2015/late-filings/Comments_510k_Coalition_Class_25.pdf; *see also* Intellectual Property Owners Association, In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems—Sixth Triennial DMCA Rulemaking—Proposed Class 26 (Mar. 27, 2015), https://www.copyright.gov/1201/2015/comments-032715/class%2026/Intellectual_Property_Owners_Association_Class26_1201_2014.pdf

more regular downloads from the implanted devices would affect the longevity and battery life of the devices, possibly requiring additional surgery to replace the batteries.[212]

FDA also opposed the granting of the exemption.[213] FDA was concerned that this may put third-party developers in a position where they might have to obtain marketing authorization before the modified device could be used by patients.[214] It also argued that patients might be confused between modified devices and original devices.[215]

In relation to implantable medical devices, the exemptions sought were divided into two classes. The first (Class 27A) concerned security research, and the second (Class 27B) related to access to patient data generated by the devices.[216] The effort achieved limited success. It resulted in an exemption to the DMCA that would allow "good faith security research" on implantable medical devices.[217] This allows circumvention of TPM's that protect the computer programs embedded in medical devices, and the monitoring devices, and in the outputs generated from the programs.[218] The exemption is limited to situations where it is at the direction of the patient who wants information from his or her own device, or is at the direction of researchers looking into safety, security, and effectiveness of the devices.[219]

This exemption for security research grants an exemption for circumvention on computer programs for "good-faith security research" when they are part of a "medical device designed for whole or partial implantation in patients or a corresponding personal monitoring system, that is not and will not be used by patients or for patient care."[220] It further goes on to define "good faith security research" as

> accessing a computer program solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability, where such activity is carried out in a controlled

("The evidentiary and legal interpretations established thus far appropriately balance the interests of intellectual property owners and users.").

212. *See* Advanced Medical Technology Association, *supra* note 12, at 2.

213. *See generally* U.S. Dep't of Health and Human Servs., *supra* note 208 ("[G]ranting such an exemption for such devices could potentially create regulatory confusion for FDA, medical device manufacturers, and third party software developers that choose to modify medical devices.").

214. *Id.* at 2.

215. *Id.* at 3.

216. 37 C.F.R § 201.40(b)(7)(i) (2017); Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65,944, 65,955 (Oct. 28, 2015).

217. *See* NAT'L TELECOMM. & INFO. ADMIN., *supra* note 101, at 89. The Copyright Office rolled Class 27 into Class 25, which was a broader security research exemption request, thus leading to the good faith exemption for that category (which happened to include medical devices). *Id.* at 88.

218. *Id.* at 59.

219. *See id.*

220. 37 C.F.R § 201.40(b)(7)(i).

> environment . . . and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.[221]

Unlike the exemption for security research, the exemption for access to patient data (Class 27B) does not permit circumvention "at the direction of a patient" as requested by the Coalition of Medical Device Researchers.[222] Instead, it reads as follows:

> Literary works consisting of compilations of data generated by medical devices that are wholly or partially implanted in the body or by their corresponding personal monitoring systems, where such circumvention is undertaken by a patient for the sole purpose of lawfully accessing the data generated by his or her own device or monitoring system and does not constitute a violation of applicable law, including without limitation the Health Insurance Portability and Accountability Act of 1996, the Computer Fraud and Abuse Act of 1986 or regulations of the Food and Drug Administration, and is accomplished through the passive monitoring of wireless transmissions that are already being produced by such device or monitoring system.[223]

It therefore only allows a more limited exemption. A patient may circumvent his own device for the purpose of accessing the data generated by the device. The circumvention must not violate other laws and must be done through passive monitoring of the wireless transmissions from the device.

In sum, from the perspective of patient advocates, the exemptions as granted represent some, albeit minimal, progress for research and access, but do not solve the problem. One exemption does allow "good faith security research" on implantable medical devices,[224] but is limited to situations where it is at the direction of the patient who wants information from his or her own device, or is at the direction of researchers looking into safety, security, and

---

221. *Id.* § 201.40(b)(7)(ii).

222. The proposed exemption read:

> Computer programs, in the form of firmware or software, including the outputs generated by those programs, that are contained within or generated by medical devices and their corresponding monitoring systems, when such devices are designated for attachment to or implantation in patients, and where such circumvention is at the direction of a patient seeking access to information generated by his or her own device or at the direction of those conducting research into the safety, security, and effectiveness of such devices.

Coalition of Medical Device Researchers, *supra* note 25, at 1.

223. 37 C.F.R § 201.40(b)(10).

224. *Id.* § 201.40(b)(7)(i).

effectiveness of the devices. The other exemption for access to patient data does not permit circumvention more broadly "at the direction of a patient,"[225] but rather permits a patient to circumvent his *own* device for the purpose of accessing the data generated by the device. Thus, as a practical matter, the only persons who appear to benefit from this exemption are those patients with implantable medical devices who happen to have the technological skill to hack into the data generated by their device. As to everyone else, the problem of real-time access remains.

C. A DISCLOSURE SPECTRUM

Recognizing the various interests discussed above, any proposed solution to sharing of data from implantable medical devices is best viewed along a spectrum where there is some sharing among the stakeholders while also protecting intellectual property rights. Determining how and what to share will be quite challenging and questions abound. For instance, does it matter the level of information requested and expertise of the recipient? Not every device is the same, nor is every recipient the same. Should consideration also be given to the type of device, along a spectrum? Should apps be treated differently from wearables, which should be treated differently from implanted devices? Should there be different treatment and levels of access for each? Should disclosure be context based?

It is important to be mindful that there are several parts to a computer program, including the source code, object code, and related files and instructions. Each may be protected and layered with intellectual property rights through patent law, copyright law, or trade secret law. It may also be useful to distinguish between raw data and the interpretation of that data.[226] The software embedded in implantable medical devices does not stand alone. In other words, manufacturers of the devices themselves need not fear that the layer of data coming from the software embedded in the device will threaten their rights or sales for the devices themselves. Arguably, though, the software could be valuable to competitors in the same space, so there remains the need to protect the source code for anti-competitive reasons.

Patients do not necessarily want access to the software on the device with respect to operability (i.e., how the device works).[227] Instead, they may just want to be able to read the data output from the device.[228] Nonetheless, any real time access to patients should not exclude the physician's role in the process. While the patient might be able to see data from the device (or some of it), the physician's role in interpreting the data and providing medical advice to the patient remains vital.

---

225. Coalition of Medical Device Researchers, *supra* note 25, at 1.
226. *See* Pasquale, *supra* note 20, at 737–38.
227. U.S. COPYRIGHT OFFICE, *supra* note 7, at 16.
228. *Id.*

Perhaps one paradigm here (albeit a less realistic one in light of the current legal landscape) might be to view patients as having a property right in their personal medical data.[229] From this perspective, the patient's control might be understood as a "bundle of sticks," including the right to exclude and the right to possession.[230] The patient would have ownership, but contracts could be created to allow the information to be used by different people for limited purposes.[231] This would allow them a stronger voice in arguing or negotiating for greater access and control. Given the status quo, however, and the relative strength of manufacturers' intellectual property rights, this may not be a realistic option for the short term.

In thinking about a property framework, it might also be worth considering whether medical data from an embedded device may be analogous to body parts, and a patient's ownership of the rights therein. As with genetic materials or organs, however, patients do not necessarily have robust ownership or property rights over their own body parts.[232] In general, a person's body parts are not treated as property in the traditional sense. Thus, for instance, people are not permitted to sell their organs. Rather, body parts are treated as gifts and donated to others. Similarly, patients do not have ownership interests in genetic materials that have been extracted from their bodies.[233]

Perhaps then the data from a patient's medical device is an *inter vivos* gift from the patient to the manufacturer. Generally, in the realm of intellectual property, if one gives information to others, or allows access and use without restrictions, it is considered a gift.[234] Is it that patients need to provide contractual language expressly stating that their data is "not a gift" and that the patient reserves his or her rights to the data? The consumer-to-business models that we have to date do not permit this kind of arrangement, so it would require legislative or judicial intervention to reframe the parties' rights.

As policymakers or courts face requests and make decisions about data sharing, it might be crucial to examine whether a request is simply for access to raw data and reports, or more intrusively, to the software and its source code for modification. For instance, a patient group was seeking an

229. *See, e.g.*, Joseph Newman, Note, *Cookie Monsters: Locally Stored Objects, User Privacy, and Section 1201 of the DMCA*, 41 AIPLA Q.J. 511, 550–51 (2013).

230. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 76–77 (2004).

231. *See* Hal R. Varian, *Economic Aspects of Personal Privacy*, NAT'L TELECOMM. & INFO. ADMIN., https://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy (last visited Aug. 5, 2018).

232. *See* Washington Univ. v. Catalona, 490 F.3d 667, 674 (8th Cir. 2007); Moore v. Regents of Univ. of Cal., 793 P.2d 479, 489 (Cal. 1990); Lori B. Andrews, *My Body, My Property*, 16 HASTINGS CTR. REP., Oct. 1986, at 28, 34.

233. *See generally* Andrews, *supra* note 232 (discussing the facts of *Moore* and people's ownership rights over their own bodies).

234. *See* ELIZABETH A. ROWE & SHARON K. SANDEEN, TRADE SECRET LAW: CASES AND MATERIALS 198–99 (2d ed. 2017).

exemption "to access the source code and the data outputs" from the device, but not to modify the software that runs the device.[235] There is, however, the realization that when one accesses the data from the device, it also implicitly provides information about how the device functions.[236] "Some patients will want to receive the entirety of the data, though they might not understand it all. However, most would do well with limited pertinent information which would serve them and their caregivers well."[237]

Another consideration might be whether safe harbors should be provided to physicians and manufacturers, in order to address liability concerns from data sharing. In this context, a safe harbor provision could set up standards with which medical device manufacturers would comply in supplying data to patients, and doing so would excuse them from legal liability. It could address the concern that information shared without the intermediary physician might be misused or misinterpreted by patients who would then seek to hold the manufacturer liable. Safe harbor provisions are not foreign to intellectual property law and could be one tool used to achieve balance between intellectual property rights and public policy concerns. One example of the existence of a safe harbor provision is DMCA section 512. This safe harbor provision protects service providers from their users' infringing activities if the providers meet certain requirements.[238] Another example of a safe harbor provision in the medical field and intellectual property is the Hatch-Waxman exemption.[239] This exemption allows for conducting research and testing in preparation for FDA approval without fear of infringing on patent rights.[240]

D. BUSINESS OR TECHNICAL SOLUTIONS

Given the complexity of the legal landscape and the notorious lack of quick and nimble solutions in the law, perhaps this problem might be best handled by the marketplace. Those manufacturers that wish to provide access to certain data may achieve a market advantage if patients and physicians end up choosing their devices over others. The question is, however, whether there is much competition in the space. There are only a few companies world-wide in this market, leading to what one report calls a "consolidated competitive landscape."[241] Therefore, in such a concentrated market, query

235. U.S. COPYRIGHT OFFICE, *supra* note 7, at 34.

236. *See id.*

237. Scher, *supra* note 160.

238. 17 U.S.C. § 512 (2012).

239. 35 U.S.C. § 271(e)(1).

240. *Id.*

241. Manufacturing Group, *Implantable Medical Devices Market's Future Growth*, TODAY'S MED. DEVS. (Mar. 15, 2017), http://www.todaysmedicaldevelopments.com/article/global-implantable-medical-device-market-2024-31517.

whether there would be any real incentive for manufacturers to provide access to data.

Given the structure of the health care delivery system in the United States, it may also be that health insurance companies are the best positioned to negotiate or require that patients with implantable devices receive real time access to their data. Given the power of contracts in this sphere, and that health insurers are the bill payers,[242] they could be in a strong bargaining position. To set foot into the fight, however, the business case would have to be made for how and why it aligns with their interests.

More and more medical apps are available on mobile phones and tablets. These apps are letting patients monitor and obtain all kinds of health data. For instance, there are onesies for infants to help monitor their heartbeat, respiration rates, and other vital signs, and all that information can be sent to the parents' phones.[243] With some apps, patients are also able to view scans and other medical images remotely, just like their physicians.[244] Consumers can even record and interpret sounds coming from their lungs, heart, and bowels.[245]

There are thousands of such apps[246] available to consumers. Accordingly, a more realistic option might be to develop apps to accompany the implantable medical devices, and that would help provide data to the patients in real time. Either the manufacturers themselves could develop these apps or allow them to be developed by third parties. This might be a way to meet the patient's interest as well as the manufacturer's interest in controlling its proprietary information. There are already apps available to consumers related to some of the very same conditions treated by implantables. For instance, there is an app that connects to a blood glucose monitoring system allowing patients to track their levels and providing alerts when sugar levels are too high or too low.[247] While these apps might have limitations[248] that make the implantable devices superior, their availability as an alternative, or their use in conjunction with implantables might be worth exploring.

---

242. *See* TANNER, *supra* note 140, at 153 ("Even though a doctor or pharmacist is providing goods or services to a patient, insurance companies . . . pay most of the bills.").

243. Fed. Trade Comm'n, FTC Spring Privacy Series: Consumer Generated and Controlled Health Data para. 12 (May 7, 2014), https://www.ftc.gov/system/files/documents/videos/spring-privacy-series-consumer-generated-controlled-health-data/ftc_spring_privacy_series_-_consumer_generated_and_controlled_health_data_-_transcript.pdf (statement of Commissioner Julie Brill).

244. *See* Nathan Cortez, *The Mobile Health Revolution?*, 47 U.C. DAVIS L. REV. 1173, 1177 (2014).

245. *Id.* at 1184.

246. *Id.* at 1178.

247. *Id.* at 1185–86 (describing iBGStar Diabetes Manager app).

248. S*ee, e.g.*, *id.* at 1210 (describing a neurostimulator app that malfunctioned).

E. EUROPEAN GUIDANCE?

Courts, policymakers, and industry in the United States have an opportunity to set the course in this cutting-edge area. Looking beyond our borders can sometimes be instructive, especially where other countries have taken the lead on difficult public policy concerns.[249] A brief look at Europe and how it might be tackling the issues raised in this Article did not yield much guidance. Indeed, the Europeans also appear to be struggling to establish new policies related to medical devices, software, and individual rights.

For instance, the European Union ("EU") recently issued the Medical Device Regulation on May 5, 2017. The two sections of the regulation deal with medical devices and in vitro diagnostic medical devices. According to the regulation,

> [i]t is necessary to clarify that software in its own right, when specifically intended by the manufacturer to be used for one or more of the medical purposes set out in the definition of a medical device, qualifies as a medical device, while software for general purposes, even when used in the healthcare setting, or software intended for life-style and well-being purposes is not a medical device.[250]

The United Kingdom does have a policy that regulates mobile health apps. The Medicines and Healthcare Products Regulatory Agency ("MHRA") published guidance related to standalone software and medical devices, including mobile health apps in March 2014.[251] It provides, among other things, that software which "has a medical purpose could be considered a medical device."[252]

Moreover, the EU passed the General Data Protection Regulation ("GDPR") in April 2016, and it took effect in May 2018.[253] It seems to provide greater rights to individuals so that they can be better informed about the use of their personal data.[254] This regulation will be applicable in all member states and seeks to define basic rights of individuals with respect to control and access of their personal data and provides common rules for data protection.[255] It looks like it might be equivalent or along the lines of HIPAA. For instance, it addresses the consent processes and privacy policies for

249. *See* Rowe, *supra* note 192, at 882.

250. Parliament and Council Regulation 2017/745, 2017 O.J. (L 117) 19 (EU).

251. Sarah Jean Kilker, Note, *Effectiveness of Federal Regulation of Mobile Medical Applications*, 93 WASH. U. L. REV. 1341, 1350 (2016).

252. *Id.*

253. Parliament and Council Regulation 2016/679, 2016 O.J. (L 119) 1.

254. *Id.* art. 12.

255. European Society of Radiology (ESR), *The New EU General Data Protection Regulation: What the Radiologist Should Know*, 8 INSIGHTS INTO IMAGING, 295, 295 (2017).

medical device manufacturers.[256] There may be potential benefit to those in the United States as well, since the GDPR also applies to U.S.-based companies by covering all EU citizens' data, regardless of where the data is collected.[257] Thus, to the extent U.S. companies make changes to comply with the GDPR for their EU citizens, those changes could inure to the benefit of U.S. consumers as well.

It also contains a provision related to data portability, which provides that patients "shall have the right to receive the personal data concerning [them] . . . in a structured, commonly used machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided."[258] This seems to suggest that patients can request data from the pacemakers or other devices that contain data.[259] It also allows patients to receive electronic data from their radiology scans upon request, so that they can consult with other providers, if desired.[260] However, it's unclear whether this provides for real-time access or something other than the ability to obtain the data from a medical provider or facility. It might mean that a patient has a right to obtain the data directly from the manufacturer, but it seems to be aimed more toward portability to another system.

VI. CONCLUSION

Millions of patients in the United States benefit from tremendous advances in medical technology, while at the same time experiencing a limitation from intellectual property law's powerful reach. This Article wrestled with the tensions presented between manufacturers and patients with respect to access to data generated from implantable medical devices. Patients argue that they may be harmed by the inability to react to data collected by their medical devices in real time, because they are forced to wait for a medical appointment with a physician.[261] These modern implantable devices are not just equipment; they can be embedded with computer processors and other sophisticated electronics.[262] Intellectual property rights along with contract law secure the rights of manufacturers to the hardware and software in those devices.[263] The fundamental ownership and access

256. Parliament and Council Regulation 2016/679, art. 12; Erik Vollebregt, *The New General Data Protection Regulation Impact on Medical Devices Industry*, MEDICALDEVICESLEGAL (May 29, 2016), https://medicaldeviceslegal.com/2016/05/29/the-new-general-data-protection-regulation-impact-on-medical-devices-industry.

257. *See* Parliament and Council Regulation 2016/679, *supra* note 242, at art. 3.

258. *Id.* art. 20.

259. Vollebregt, *supra* note 245.

260. *See* European Society of Radiology, *supra* note 255, at 297.

261. *See supra* Section IV.A.2.

262. *See supra* Section II.B.

263. *See supra* Part III.

questions begin with the hardware. To the extent patients may have a claim for ownership under the current legal landscape, it might be with the hardware.[264] With respect to the software, however, manufacturers own the intellectual property in the software that runs the device and arguably also the data generated from it.[265] As such, they can control who has access to the data and the level of access. Patients do not have access to the data, and reports from the data (not necessarily the data itself) are provided only to the physician or medical facility.[266] Patients also do not control what could happen to the information collected from their devices.[267]

The Article argues that, ultimately, it is important to determine how to achieve the appropriate balance among the various constituents and their respective interests. Manufacturers' desire to protect their intellectual property rights is reasonable, and trade secrets in their software and data ought to be safeguarded. Cybersecurity and other safety concerns have motivated patients and researchers to seek a security research exemption under copyright law, as well as access to patient data.[268] While a limited exemption was recently allowed for good faith security research, an exemption for patient data essentially only allows a patient to passively monitor wireless transmissions from his own device—an outcome that arguable benefits only patients with hacking skills.[269]

The Article recommends a disclosure spectrum from which to frame the sharing of information, one that takes a more nuanced approach to what might be shared.[270] Determining how and what to share is challenging and the Article suggests a closer inquiry into the nature and scope of the data requested in arriving at an appropriate response. For instance, it might be crucial to examine whether a request is simply for access to raw data and reports, or more intrusively, to the software and its source code. Market and technological solutions such as the use of manufacturer-sanctioned apps that work in conjunction with the implantable devices to provide access to data, were also explored.[271] In the end, more careful consideration of the parties' respective interests might lead to more amicable and workable solutions as we move through our digitally interconnected world.

264. *See supra* Section II.C.
265. *See supra* Section II.C.
266. *See supra* Section II.C.
267. *See supra* Section II.C.
268. *See supra* Section IV.A.2–3.
269. *See supra* Section V.B.
270. *See supra* Section V.C.
271. *See supra* Section V.D.