University of Pennsylvania Carey Law School

ILE

INSTITUTE FOR LAW AND ECONOMICS

A Joint Research Center of the Law School, the Wharton School,
and the Department of Economics in the School of Arts and Sciences
at the University of Pennsylvania

RESEARCH PAPER NO. 22-20

Optimizing Cybersecurity Risk in Medical Cyber-Physical Devices

Christopher S. Yoo
UNIVERSITY OF PENNSYLVANIA CAREY LAW SCHOOL

Bethany Lee
UNIVERSITY OF PENNSYLVANIA CAREY LAW SCHOOL

Optimizing Cybersecurity Risk in Medical Cyber-Physical Devices

Christopher S. Yoo* and Bethany C. Lee**

ABSTRACT

Medical devices are increasingly connected, both to cyber networks and to sensors collecting data from physical stimuli. These cyber-physical systems pose a new host of deadly security risks that traditional notions of cybersecurity struggle to take into account. Previously, we could predict how algorithms would function as they drew on defined inputs. But cyber-physical systems draw on unbounded inputs from the real world. Moreover, with wide networks of cyber-physical medical devices, a single cybersecurity breach could pose lethal dangers to masses of patients.

The U.S. Food and Drug Administration (FDA) is tasked with regulating medical devices to ensure safety and effectiveness, but its regulatory approach—designed decades ago to regulate traditional medical hardware—is ill-suited to the unique problems of cybersecurity. Because perfect cybersecurity is impossible and every cybersecurity improvement entails costs to affordability and health, designers need standards that balance costs and benefits to inform the optimal level of risk. FDA, however, conducts limited cost-benefit analyses, believing that its authorizing statute forbids consideration of economic costs.

We draw on statutory text and case law to show that this belief is mistaken and that FDA can and should conduct cost-benefit analyses to ensure safety and effectiveness, especially in the context of cybersecurity. We describe three approaches FDA could take to implement this analysis as a practical matter. Of these three, we recommend an approach modeled after the Federal Trade Commission's cost-benefit test. Regardless of the specific approach FDA chooses, however, the critical point is that the agency must weigh costs and benefits to ensure the right level of cybersecurity. Until then, medical device designers will face continued uncertainty as cybersecurity threats become increasingly dangerous.

---

* John H. Chestnut Professor of Law, Communication, and Computer & Information Science and Founding Director of the Center for Technology, Innovation and Competition, University of Pennsylvania.

** M.P.H. in Epidemiology & Biostatistics, University of California, Berkeley; J.D. Candidate, 2022, University of Pennsylvania Carey Law School. We thank James Park and Allie Cohen for valuable contributions to this research. This research was supported in part by NSF CNS-1505799 and the Intel-NSF Partnership for Cyber-Physical Systems Security and Privacy. All opinions, errors, and omissions are the responsibility of the authors.

TABLE OF CONTENTS

INTRODUCTION

"Yes, terrorists could have hacked Dick Cheney's heart."[1] The former vice president's heart implant, with its wireless functionality, could have resulted in an assassination.[2] Recognizing this possibility, Cheney's doctor had to order the wireless functionality of the heart implant to be disabled.[3]

Cheney's story is just one example of the risk of deadly cybersecurity attacks on connected medical devices. Numerous other reports and studies have shown how cybersecurity threats endanger lives.[4] Researchers have shown that a hacker can remotely kill a person by causing an implanted insulin pump to release a deadly dose of insulin or by making a pacemaker release a heart-stopping electric charge.[5]

---

[1] Andrea Peterson, *Yes, Terrorists Could Have Hacked Dick Cheney's Heart*, WASH. POST (Oct. 21, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/.

[2] *Id.*

[3] *Id.*

[4] *See, e.g.*, Susan D. Hall, *Hospital Medical Devices Riddled with Malware*, FIERCE HEALTH IT (Oct. 18, 2012), http://www.fiercehealthit.com/story/hospital-medical-devices-riddledmalware/2012-10-18.9 (reporting that hackers have increasingly attacked medical devices, affecting everything from glucose monitors to sleep labs); Press Release, U.S. Atty's Off., N.D. Tex., *Former Security Guard Who Hacked Into Hospital's Computer System Sentenced to 110 Months in Federal Prison* (Mar. 18, 2011), http://www.fbi.gov/dallas/press-releases/2011/dl031811.htm (reporting on the hacking of a hospital's computer system through transmission of malicious code); John Leyden, *Paging Dr. Evil: Philips Medical Device Control Kit 'Easily Hacked,'* REGISTER (Jan. 18, 2013, 5:03 PM), http://www.theregister.co.uk/2013/01/18/medical_device_control_kit_security (showing that hackers could access a medical management platform and operate any medical device connected to the platform); *see also* U.S. DEP'T OF HOMELAND SEC., NAT'L CYBERSECURITY & COMMC'NS INTEGRATION CTR., ATTACK SURFACE: HEALTHCARE AND PUBLIC HEALTH SECTOR 3 (2012), http://info.publicintelligence.net/NCCIC-MedicalDevices.pdf (stating that medical information can be remotely stolen from medical devices).

[5] Christine Hsu, *Many Popular Medical Devices May Be Vulnerable to Cyber Attacks*, MED. DAILY (Apr. 10, 2012, 1:34 PM), http://www.medicaldaily.com/news/20120410/9486/medical-implants-pacemaker-hackerscyber-attack-fda.htm; Tarun Wadhwa, *Yes, You Can Hack a Pacemaker (and Other Medical Devices Too),* FORBES (Dec. 6, 2012, 8:31 AM), http://www.forbes.com/sites/singularity/2012/12/06/yes-youcan-hack-a-pacemaker-and-other-medical-devices-too; Nathanael Paul et al., *A Review of the Security of Insulin Pump Infusion Systems*, 5 J. DIABETES SCI. & TECH. 1557 (2011), http://www.ncbi.nlm.nih.gov/pmc/articles/ PMC3262727 (showing that hackers can gain remote access to an insulin pump from 100 feet away). Though no patient harm from cyberattacks on medical devices have been documented, close calls have happened. Katherine Wellington, *Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions*, 30 SANTA CLARA HIGH TECH. L.J. 139, 146 (2014).

These connected medical devices present special cybersecurity risks because they are part of cyber-physical systems. In cyber-physical systems, devices not only interact with other networked devices but also receive and respond to input from the physical environment. Other prominent examples include autonomous vehicles, smart grid sensors, and robotics systems.

In an increasingly cyber-physical world, traditional notions of cybersecurity fall short. When devices were purely cyber, the predefined nature of the inputs they could receive made their behavior easier to predict and different systems' responses to those inputs easier to validate. The data fed into cyber-physical systems are not so rigidly constrained, as the physical environment involves real-world events that are theoretically unbounded and do not always stay within predictable limits. Body temperature, for example, almost always stays within a certain range, yet unprecedented readings can and do occur.[6] The unbounded nature of the data prevents designers from testing how a cyber-physical device will function in every possible real-world scenario, making it impossible to rule out black swan events with low probability but high impact.

In addition, threats to medical cyber-physical devices often involve the deliberate actions by malicious actors whose novel attacks cannot always be anticipated. The fact that cyber-physical systems can be networked across hospitals and third-party institutions raises the stakes still further. The large user base increases the probability of breaches as well as the potential magnitude of the resulting harm. As malicious actors constantly invent new zero-day attacks, designers must plan for ever-evolving changes to cybersecurity needs.

---

[6] *See, e.g.*, Mads Gilbert et al., *Resuscitation from Accidental Hypothermia of 13.7C with Circulatory Arrest*, 355 LANCET 9201 (2000), https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(00)01021-7/fulltext (describing a record-breaking drop in body temperature).

The inability to eliminate cybersecurity risks completely means that a designer can always add additional security features to plan for an ever-broader range of scenarios. Each increase in cybersecurity comes at a cost. Besides the obvious monetary cost, the additional processing power, storage, and battery power that new cybersecurity features require may hinder a device's functionality, posing costs to health. For example, a security feature that increases the size of a device or increase its power consumption could make the device more dangerous or reduce its effectiveness as a bodily implant. In a world of limited resources, additional security improvements must end at some point.

Since designers cannot proactively eliminate every cybersecurity flaw, they need a framework for determining what constitutes an acceptable level of risk to determine when they can stop adding security. Cybersecurity thus inevitably requires some type of cost-benefit analysis to inform the optimal level of cybersecurity.

Federal regulators, however, have offered no such solution in defining cybersecurity standards for medical devices. The U.S. Food & Drug Administration ("FDA"), which regulates medical devices, offers only nonbinding guidance documents recommending certain cybersecurity features.[7] Moreover, these documents do not address the optimal level of security or make any mention of cost considerations. In fact, FDA has interpreted its own authority in a limited way, operating on an internal policy that the agency cannot consider financial costs when evaluating products.[8]

---

[7] *Cybersecurity*, FOOD & DRUG ADMIN. (Dec. 22, 2021), https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.

[8] *See, e.g.*, Sarah Duranske, *This Article Makes You Smarter! (or, Regulating Health and Wellness Claims)*, 43 AM. J.L. & MED. 7, 25 (2017) ("In determining whether to approve or clear a medical device, the FDA considers evidence of safety and effectiveness. But other potential consumer harms—like economic harms—are not accounted for in FDA regulation."); *id.* at 47 ("The FDA evaluates products based on their safety and effectiveness, and does not factor economic considerations into its analysis.").

The inadequacy of FDA's cybersecurity regulation is just one symptom of its troubling record with software. Commentators have long noted that FDA's overarching regulatory approach is ill fitted for software, creating difficulties for designers of medical device software.[9] Having abandoned multiple attempts to create a separate approach to software, FDA seems to know that it has a problem with software and cybersecurity regulation.[10] But the agency has yet to address the issue.

A logical solution for the agency would involve some type of cost-benefit analysis to inform the optimal level of cybersecurity risk, but FDA does not conduct economic cost-benefit analyses. Instead, FDA has interpreted its authorizing statute as prohibiting consideration of economic costs, inhibiting the agency's ability to weigh these costs with benefits.[11]

The agency's resulting approach to cybersecurity means a lack of clarity for medical device designers and potentially unsafe or inefficient devices. This Essay tackles this problem by recommending approaches that FDA can use to define the optimal level of cybersecurity, taking into account the costs and benefits of potential cybersecurity features.

This Essay proceeds in three parts. Part I highlights the unique challenges of medical device cybersecurity and their poor fit within existing regulatory approaches. Part II examines the existing legal constraints on FDA's ability to set standards that balance costs and benefits.

---

[9] *See, e.g.*, Bruce Merlin Fried & Jason Mark Zuckerman, *FDA Regulation of Medical Software*, 33 J. HEALTH L. 129, 129 (2000) (noting that twenty years of FDA regulation of software had left the medical software industry in a state of "uncertainty and confusion"); Komal Karnik, *FDA Regulation if Clinical Decision Support Software*, 1 J.L. & BIOSCIENCES 202, 204 (2014) (noting that FDA has enjoyed "little success" regulating software); Vincent J. Roth, *The MHealth Conundrum: Smartphones & Mobile Medical Apps--How Much FDA Medical Device Regulation Is Required?*, 15 N.C. J.L. & TECH. 359, 378 (2014) (noting that "[s]oftware presents a challenge to the FDA"); Ann K. Schooley, Note, *Allowing FDA Regulation of Communications Software Used in Telemedicine: A Potentially Fatal Misdiagnosis?*, 50 FED. COMM. L.J. 731, 744 (1998) (noting that the "[t]he lack of guidance from the FDA poses a huge problem" for the medical software industry).

[10] *Id.*

[11] *See supra* note 8 and accompanying text.

Drawing from statutory text and case law, we argue that FDA can in fact weigh economic costs when evaluating products and that doing so is particularly important in the context of cybersecurity. Finally, Part III discusses three potential approaches FDA can implement to determine the optimal level of cybersecurity. We explore the implications of each approach and conclude that FDA's best option is to adopt the cost-benefit test used by the Federal Trade Commission ("FTC"). Regardless of which option FDA chooses, however, the crucial point is that FDA must use a balancing test that ensures the optimal level of cybersecurity in medical devices.

I. THE UNIQUE PROBLEMS OF SOFTWARE AND CYBERSECURITY IN MEDICAL DEVICE REGULATION

Cybersecurity is a far cry from the traditional medical risks that FDA regulates. As a result, FDA's regulatory framework provides an insufficient approach for optimizing medical device cybersecurity.

FDA's troubling record with cybersecurity is no surprise given the agency's troubling record with software in general. FDA's regulation of medical devices originated in a time when devices included insubstantial software.[12] As one expert testified to Congress, FDA staff saw software as "some kind of new bedpan."[13] Since then, software has come to play significant roles in medical devices. But despite radical differences between software and traditional hardware,

---

[12] Benjamin M. Zegarelli & Lara D. Compton, *Coverage of FDA's AI/ML Medical Devices Workshop – Part 1: The History of FDA Software Regulation*, MINTZ (Oct. 4, 2021), https://www.mintz.com/insights-center/viewpoints/2791/2021-10-04-coverage-fdas-aiml-medical-devices-workshop-part-1.

[13] *Information Technologies in the Health Care System: Hearing Before the Subcomm. on Investigations and Oversight of the H. Comm. on Sci. and Tech.*, 99th Cong. 167 (1986) (statement of Vincent Brannigan, Associate Professor of Consumer Law, University of Maryland), *cited in* Nathan Cortez, *Digital Health and Regulatory Experimentation at the FDA*, 21 YALE J.L. & TECH. 4, 6 (2019).

FDA continues to regulate both under the same framework, "like forcing a round peg into a square hole."[14] As a result, FDA's regulation of software has often left medical software developers in a state of confusion.[15]

The current framework for FDA regulation of medical devices traces back to the Medical Device Amendments of 1976.[16] The statute established three classes of devices based on risk, with Class I devices posing the lowest risks and Class III posing the highest risk.[17] Software, however, was not seen as a major element of patient care. As medical devices increasingly transitioned from consisting only of hardware to incorporating software as critical elements of the device, FDA began to recognize the challenges of software, noting in 1996 that an agency study of software-related recalls from fiscal years 1983 to 1991 revealed that "over 90 percent of all software-related device failures were due to design-related errors."[18]

FDA's approach to software regulation presents many problems given the differences between software and hardware. For example, hardware devices tend to have an easily defined purpose, while software can have numerous and interdependent intended uses, both related and

---

[14] Zegarelli & Compton, *supra* note 9.
[15] *See, e.g.*, Fried & Zuckerman, *supra* note 9, at 129 ("Since the passage of the 1976 Medical Device Amendments to the Federal Food, Drug and Cosmetic Act ('FFDCA'), the medical software industry has experienced uncertainty and confusion concerning FDA regulation of software products."); Schooley, *supra* note 9 at 744 ("The lack of guidance from the FDA poses a huge problem for those developing such systems, for those manufacturing components of the systems, and for those health care providers purchasing a system—only to later find out it does not comply with newly created FDA regulations").
[16] Pub. L. No. 94-295, 90 Stat. 539 (1976). The original Food, Drug and Cosmetic Act enacted in 1938 gave FDA some limited authority to regulate medical devices, but that authority was soon found to be inadequate. Sara Lykken, *We Really Need to Talk: Adapting FDA Processes to Rapid Change*,68 FOOD & DRUG L.J. 357, 365-66 (2013); Marilyn Uzdavines, *Dying for a Solution: The Regulation of Medical Devices Falls Short in the 21st Century CURES Act*, 18 NEV. L.J. 629, 637-39 (2018).
[17] 21 U.S.C. § 360c(a)(1); *see also Overview of Medical Device Classification and Reclassification*, FOOD & DRUG ADMIN. (Dec. 19, 2017), https://www.fda.gov/about-fda/cdrh-transparency/overview-medical-device-classification-and-reclassification.
[18] Medical Devices; Current Good Manufacturing Practice (CGMP) Final Rule; Quality System Regulation, 61 Fed. Reg. 52,602, 52,602 (Oct. 7, 1996).

unrelated to the medical device.[19] These multiple functionalities fit uneasily within FDA's regulatory approach. Furthermore, Class II medical devices must receive a determination of substantial equivalence to an already-approved device, but it is difficult to compare new software products with multiple functionalities to their "equivalent" hardware products.[20] In addition, many of the quality controls applicable for device hardware—such as packing, storage, or distribution—do not apply to software.[21]

The need for frequent updates is another unique attribute of software that does not fit well within FDA's framework.[22] FDA requires new approval for any device that undergoes "significant changes or modifications" that affect the safety, effectiveness, or intended uses of the device.[23] For hardware devices, seeking new approval makes sense for new releases that involve significant bundled developments. But with software, which may be modified quickly and released with incremental updates, the need to seek re-approval for every update is unrealistic. FDA has issued guidance attempting to clarify when software updates necessitate new approval from the agency,[24] but the process has remained unwieldy and confusing for software developers.

---

[19] FOOD & DRUG ADMIN., POLICY FOR DEVICE SOFTWARE FUNCTIONS AND MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 1 (Sept. 27, 2019), https://www.fda.gov/media/80958/download [hereinafter 2019 FDA SOFTWARE FUNCTIONS GUIDANCE] (observing that software may be used either *as* a medical device or *in* a medical device).
[20] Zegarelli & Compton, *supra* note 9.
[21] *See, e.g.*, 21 C.F.R. § 814.80 ("A device may not be manufactured, packaged, stored, labeled, distributed, or advertised in a manner that is inconsistent with any conditions to approval specified in the PMA approval order for the device."); Zegarelli & Compton, *supra* note 9.
[22] Schooley, *supra* note 15, at 749 ("Software manufacturers or developers are in an especially problematic position to deal with FDA regulation. With each new version of the software, new FDA approval would be necessary. Every change to eliminate a bug in the program could potentially require additional FDA approval.").
[23] 21 C.F.R. § 807.81(a)(3); *Is a new 510(k) required for a modification to the device?*, FOOD & DRUG ADMIN. (Oct. 31, 2017), https://www.fda.gov/medical-devices/premarket-notification-510k/new-510k-required-modification-device.
[24] FOOD & DRUG ADMIN., DECIDING WHEN TO SUBMIT A 510(K) FOR A SOFTWARE CHANGE TO AN EXISTING DEVICE: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (Oct. 25, 2017), https://www.fda.gov/media/99785/download.

Beyond the general problems with software regulation, cybersecurity in particular presents unique challenges that are hard to incorporate into FDA's general framework. With most FDA-evaluated products, such as food and drugs, safety concerns are merely a function of statistical probability—for example, the likelihood of side effects. But with cybersecurity, harm can be caused by malicious actors. Since the plans and innovations of malicious actors cannot be reduced to a statistical probability, FDA cannot enforce its typical standard of "safety" by requiring the likelihood of cyberattacks to be under a certain level.

Furthermore, because perfect cybersecurity is impossible no matter how much a designer invests in protective measures, a notion of acceptable risk is inevitable. A workable framework for cybersecurity would thus need to incorporate some type of cost-benefit analysis to inform an acceptable level of risk.

II. Legal Framework Governing FDA's Consideration of Nontherapeutic Costs

The ongoing problems with FDA's regulation of cybersecurity call for some type of cost-benefit analysis to inform an acceptable level of cybersecurity risk. Despite this logical need, commentators have long observed that FDA does not consider economic costs in evaluating devices.[25] FDA has developed this internal policy based on its interpretation that the agency's authorizing statute forbids consideration of economic costs.

FDA receives its authority to regulate medical devices from the Federal Food, Drug & Cosmetic Act ("FDCA").[26] The current version of the FDCA gives FDA the mission and obligation to ensure that there is "reasonable assurance of the safety and effectiveness" of

[25] *See supra* note 8 and accompanying text.
[26] 21 U.S.C. §§ 351-360; *Overview of Device Regulation: Code of Federal Regulations*, *supra* note 17.

medical devices."[27] The statute further provides that "the safety and effectiveness of a device are to be determined . . . weighing any probable benefit to health from the use of the device against any probable risk of injury or illness from such use."[28]

For medical devices generally, FDA defines a reasonable assurance of safety as "valid scientific evidence that the probable benefits to health from use of the device for its intended uses . . . outweigh any probable risks."[29] Likewise, a reasonable assurance of effectiveness requires "valid scientific evidence that in a significant portion of the target population, the use of the device for its intended uses . . . will provide clinically significant results."[30] FDA has interpreted this authority as requiring it to evaluate the benefit-risk profile of medical devices solely from a scientific perspective by assessing the types, magnitude, probability, and duration of probable health benefits and risks along with the risk of false positives and negatives.[31] The Supreme Court has recognized that the FDCA "generally requires the FDA to prevent the marketing of any drug or device where the 'potential for inflicting death or physical injury is not offset by the possibility of therapeutic benefit.'"[32] The Court has also invoked the benefits of FDA's balancing of the health-related risks and benefits of medical devices as a justification

---

[27] 21 U.S.C. §§ 360c(a)(1)(A)(i)-(ii), (B), (C)(i), 393(b)(2)(C).

[28] *Id.* § 360c(2)(C).
[29] FOOD & DRUG ADMIN., PMA CLINICAL STUDIES (May 22, 2020), https://www.fda.gov/medical-devices/premarket-approval-pma/pma-clinical-studies.
[30] *Id.*
[31] FOOD & DRUG ADMIN., FACTORS TO CONSIDER WHEN MAKING BENEFIT-RISK DETERMINATIONS IN MEDICAL DEVICE PREMARKET APPROVAL AND DE NOVO CLASSIFICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 8-11 (Aug. 30, 2019), https://www.fda.gov/media/99769/download.
[32] FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 134 (2000) (quoting United States v. Rutherford, 442. U.S. 544, 556 (1979)).

supporting the preemption of state tort law, since tort law cases would be decided by juries that would not necessarily conduct such cost-benefit analysis.[33]

The historical context that gave rise to the FDCA helps explain its emphasis on safety and effectiveness. Motivated by high-profile deaths caused by adulterated and improperly formulated drugs, the FDCA as originally enacted in 1938 and its predecessor statutes focused exclusively on the safety of drugs and, to a limited extent, medical devices.[34] Congress imposed additional safety requirements and new effectiveness requirements in 1962 in response to deaths and birth defects caused by the tranquilizer thalidomide in Europe.[35] These safety requirements reflected ideas intuitive with traditional drugs: society does not want drugs that will harm people or fail to treat as advertised. Driven by the inadequacy of the existing regime for regulating medical devices, particularly in light of the injuries caused by the Dalkon Shield, the Medical Device Amendments of 1976 created a more comprehensive regime for regulating devices.[36]

Although FDA balances health-related benefits and risks, it has consistently regarded itself as limited to scientific considerations and has thus regarded economic considerations as falling outside its statutory mandate.[37] In the words of a former FDA chief counsel: "If a new

---

[33] 552 U.S. 312, 325 (2008) ("A state statute, or a regulation adopted by a state agency, could at least be expected to apply cost-benefit analysis similar to that applied by the experts at the FDA: How many more lives will be saved by a device which, along with its greater effectiveness, brings a greater risk of harm?").
[34] Elizabeth M. Rutherford, *The FDA and "Privatization"—The Drug Approval Process*, 50 FOOD & DRUG L.J. 203, 212 (1995) (describing how deaths caused by tetanus-infected diphtheria antitoxins led to the enactment of the Biologics Act of 1902 and how the inclusion of diethylene glycol in Elixir Sulfanilamide led to the enactment of the FDCA).
[35] AGATA DABROWSKA & SUSAN THAUL, CONG. RSCH. SERV., HOW FDA APPROVES DRUGS AND REGULATES THEIR SAFETY AND EFFECTIVENESS 1-2 (2012), *available at* https://sgp.fas.org/crs/misc/R41983.pdf; OFF. OF TECH. ASSESSMENT, THE IMPLICATIONS OF COST-EFFECTIVENESS ANALYSIS OF MEDICAL TECHNOLOGY 85 (Aug. 1980), *available at* https://www.princeton.edu/~ota/disk3/1980/8011/8011.PDF; Rutherford, *supra* note 34, at 212.
[36] *Riegel*, 552 U.S. at 335-36 (Ginsburg, J., dissenting); Uzdavines, *supra* note 16, at 639-41.
[37] *See, e.g.*, *FDA's Response to Public Comments on Draft Guidance for Industry #187*, FOOD & DRUG ADMIN. (Sept. 18, 2018), https://www.fda.gov/animal-veterinary/animals-intentional-genomic-alterations/fdas-response-public-comments-draft-guidance-industry-187-released-9182008 (concluding that "social and economic

drug is shown to be safe, effective, and properly manufactured and labeled, it cannot properly be denied approval on the ground, say, that it will be expensive and cause financial problems for consumers and third-party payers."[38] From this perspective, "FDA . . . best serves [its] mission by reviewing product applications and regulating approved products in accordance with the well-understood statutory standards, by making decisions promptly, and by leaving product selection and the culture wars to the free choices of free Americans."[39] Consistent with this view, "[o]ften the FDA will leave drugs on the market even if they do cause risks because there are no safer product alternatives that produce the same level of benefit."[40] Once a drug or device passes the statutory thresholds of safety and efficacy, the ultimate decision rests with patients advised by their physicians. And on the rare occasions when FDA has considered economic information in order to regulate cost-effectiveness claims by pharmaceutical companies, it has held these claims to the clinical standard for effectiveness, which requires two adequate and well-controlled studies, even though economic evidence that meets such a standard can be difficult or impossible to collect.[41]

FDA's refusal to consider economic considerations has come under increasing criticism in recent years. For example, some argue that the refusal to consider cost has contributed to the

---

consequences" fall "largely outside the scope of FDA's authority"); FOOD & DRUG ADMIN., FDA OVERVIEW OF ISSUES FOR THE JOINT NONPRESCRIPTION DRUGS ADVISORY COMMITTEE AND THE PULMONARY-ALLERGY DRUGS ADVISORY COMMITTEE (2001), https://wayback.archive-it.org/7993/20170405172117/https://www.fda.gov/ohrms/dockets/ac/01/briefing/3737b_02_overview.pdf (declining to accept comments on "economic considerations" because "these are not the purview of the FDA").

[38] Richard M. Cooper, *Science, Ethics and Economics in FDA Decision-Making: The Legal Framework*, 61 FOOD & DRUG L.J. 799, 801 (2006).

[39] *Id.* at 803.

[40] Richard A. Epstein, *Why the FDA Must Preempt Tort Litigation: A Critique of Chevron Defense and a Response to Richard Nagareda*, 1 J. TORT L. 5, 23 (2006).

[41] Note, *Will Health Care Economic Information Lead to Therapeutic-Class Warfare or Welfare*, 111 HARV. L. REV. 2384, 2385 (1998); *see also* Peter J. Neumann, Darren E. Zinner & A. David Paltiel, *The FDA and Regulation of Cost-Effectiveness Claims*, HEALTH AFF., Fall 1996 at 54, 55-60 (discussing FDA's regulation of pharmacoeconomic claims by pharmaceutical companies).

rise in drug prices, as many insurers reimburse any drug approved by FDA without assessing whether it is inferior or cost effective.[42]

FDA's latitude to take purely economic considerations into account is unclear. The Office of Technology Assessment observed in 1980 that the FDCA "neither authorizes nor prohibits the consideration of economic criteria in FDA's evaluation of applicant drugs and devices" and that "[t]he legality of using cost effectiveness to help evaluate new drugs and devices has not been tested."[43] Since that time, a broad range of legal doctrines have emerged that shed new light on how to construe statutes in the face of such ambiguity. First, we consider whether other provisions of the FDCA implicitly prohibit consideration of costs. Second, we evaluate whether the FDCA's requirement of a reasonable assurance of safety and effectiveness is ambiguous about whether FDA can consider of costs, justifying *Chevron* deference. Third, we argue that even rejecting FDA's general authority to consider costs, FDA still has authority to consider costs in the context of cybersecurity, which does not fit well within FDA's traditional frameworks.

A. Prohibition of Cost Considerations

The Supreme Court has found implicit statutory prohibition of cost considerations in limited circumstances. In *Whitman v. American Trucking Associations*, the Court interpreted a requirement in the Clean Air Act as implicitly prohibiting consideration of cost.[44] The Act instructed the Environmental Protection Agency ("EPA") to set ambient air quality standards that

---

[42] Diana M. Zuckerman, *Can the FDA Help Reduce Drug Prices or the Cost of Medical Care?*, 107 AM. J. PUB. HEALTH 1752, 1753 (2017), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5637698/.
[43] OFF. OF TECH. ASSESSMENT, *supra* note 35, at 88-89.
[44] 531 U.S. 457, 464-76 (2001).

"are requisite to protect the public health," "allowing an adequate margin of safety."[45] The Court held that this standard prohibited consideration of costs because the language was "absolute" and because "[n]owhere are the costs of achieving such a standard made part of that initial calculation."[46] Indeed, "Congress was unquestionably aware" that "the economic cost of implementing a very stringent standard might produce health losses sufficient to offset the health gains achieved in cleaning the air," but instead of including a provision requiring consideration of economic costs, it included a provision requiring a comprehensive study and provided for a waiver process if necessary.[47]

The Court drew the opposite conclusion in *Entergy Corp. v. Riverkeeper, Inc.* when analyzing language in the Clean Water Act requiring the EPA to set standards "minimizing adverse environmental impact."[48] The Court compared this language with other parts of the statute that called for "elimination of discharges of all pollutants."[49] Because the "minimizing" language was more relative and ambiguous that the "elimination" language, the Court concluded that the directive to minimize adverse environmental impact did not prohibit the EPA from conducting cost-benefit analyses.[50]

---

[45] *Id.* at 472.
[46] *Id.* at 464-65 (quoting DAVID CURRIE, AIR POLLUTION: FEDERAL LAW AND ANALYSIS 4-15 (1981)); *accord* Richard J. Pierce Jr., *What Factors Can an Agency Consider in Making a Decision?*, 2009 MICH. ST. L. REV. 67 (2009) (agreeing that the statute required EPA to "ignore the costs of alternative standards and to set a standard that protects the public health even if the costs of the standard exceed its benefits").
[47] *Whitman*, 531 U.S. at 466-67.
[48] 556 U.S. 208, 219-20 (2009).
[49] *Id.* at 219 (comparing "elimination" language in other parts of the statute with "the less ambitious goal" of minimization).
[50] *Id.* ("[T]he phrase 'best technology available,' even with the added specification 'for minimizing adverse environmental impact,' does not unambiguously preclude cost-benefit analysis.").

Although some have suggested that the lack of express authorization implies the contrary,[51] we argue that FDA's consideration of costs would be unlike the *Whitman* scenario, in which consideration of costs would have created exceptions to the Clean Air Act's provision requiring standards "requisite to protect the public" and would have contradicted Congress's decision to address any cost-related concerns through comprehensive study and a potential waiver process.[52] Here, FDA's consideration of costs would not create any exceptions to the FDCA's "reasonable assurance of safety and effectiveness" standard.[53] Rather, cost would be one factor in a balancing test to determine the reasonable assurance of safety that the statute calls for. For example, if a feature of a medical device provided a slight contribution to safety but imposed exorbitant costs, the feature would not be necessary for a reasonable assurance of safety.

This conclusion draws further support from an amendment to the FDCA known as the Delaney Clause, which forbids FDA from approving certain food additives "found to induce cancer when ingested by man or animals."[54] The D.C. Circuit interpreted the Delaney Clause as forbidding FDA from considering costs or benefits in deciding whether to allow an animal carcinogen as a food additive,[55] despite the fact that "many substances that induce cancer in

---

[51] Former FDA Chief Counsel Richard Cooper opines:

> The very fact that the legal authorities that govern FDA expressly require consideration of science, ethics, and economics in some circumstances supports an arguable inference that those legal authorities also, by plain implication, exclude consideration of such factors in other circumstances. . . . If a new drug is shown to be safe, effective, and properly manufactured and labeled, it cannot properly be denied approval on the ground, say, that it will be expensive and cause financial problems for consumers and third-party payers.

Cooper, *supra* note 38, at 801.
[52] *Whitman*, 531 U.S. at 468-69.
[53] 21 U.S.C. § 360c.
[54] 21 U.S.C. §§ 348(c)(3), 376(b)(5)(B); *see also* Richard Merrill, *Regulating Carcinogens in Food: A Legislator's Guide to the Food Safety Provisions of the Federal Food, Drug and Cosmetic Act*, 77 MICH. L. REV. 171 (1978) (discussing interpretations of the Delaney Clause).
[55] Pub. Citizen v. Young, 831 F.2d 1108 (D.C. Cir. 1987); Les v. Reilly, 968 F.2d 985 (9th Cir. 1992).

animals are safer for human consumption than many substances that are regularly ingested by humans."[56] If FDA were allowed to consider costs, this would create exceptions to the explicit prohibition against cancer-inducing food products.

The inclusion of the Delaney Clause in the FDCA shows that Congress knows how to categorically prohibit FDA from considering costs when it believes that doing so is important. Yet, when instructing FDA to set standards for safety and effectiveness, Congress chose more ambiguous and indefinite language, requiring "reasonable assurance" instead of making categorical prohibitions. This implies that Congress did not intend to prohibit FDA from considering costs when setting standards for safety and effectiveness. Instead of imposing a categorical prohibition, Congress employed a much more flexible standard requiring FDA to provide "a reasonable assurance of safety and effectiveness." Construing this language as prohibiting consideration of cost would not only be inconsistent with the Delaney Clause; it would contradict Congress's use of the word "reasonable," which necessarily requires the consideration of multiple factors in some form of balancing. No case law indicates that costs are a prohibited factor when a statute calls for reasonable assurance.

B. Statutory Ambiguity

Statutory silence on economic cost provides leeway for FDA to consider it. Agencies typically receive *Chevron* deference when construing ambiguities or statutory gaps in the statutes they administer.[57] An agency "speaks with the force of law" when it addresses an ambiguity or gap in a statute, even if Congress had no actual intent as to a particular result.[58] The Court has

---

[56] Pierce, *supra* note 46, at 71-72.
[57] United States v. Mead Corp., 533 U.S. 218, 229 (2001).
[58] *Id*.

accorded *Chevron* deference to FDA constructions of the FDCA.[59] Since the FDCA contains no explicit prohibition on considering cost, the pertinent question is whether construing "reasonable assurance of safety and effectiveness" to include consideration of costs would survive scrutiny under *Chevron*.

Similar terms have been read by the Supreme Court not just to allow but to require consideration of cost. For example, the Court has interpreted the "appropriate and necessary" standard in the Clean Air Act as requiring the EPA to consider cost,[60] and a "reasonable" standard here could carry a similar connotation. Lower courts have also suggested that the word "reasonable" contains ambiguity. For example, when analyzing "reasonable costs" as defined in the Social Security Act,[61] courts have concluded that this phrase has ambiguous language, which agencies have broad discretion to interpret.[62]

FDA could argue that consideration of economic costs is inherent to the FDCA's reasonableness standard. The word "reasonable" must be construed to include consideration of costs, since an assurance of safety and effectiveness that requires impractical costs would not be reasonable. At a minimum, "reasonable assurance" constitutes an ambiguous statutory term, to

---

[59] *See, e.g.*, Young v. Cmty. Nutrition Inst., 476 U.S. 974, 980 (1986); Hillsborough Cmty. v. Automated Med. Labs., Inc., 471 U.S. 707, 714-15 (1985). *But see* FDA v. Brown & Williamson Tobacco Corp. 529 U.S. 120, 133-61 (2000) (refusing to extend *Chevron* deference to FDA constructions where the FDCA as a whole and other legislation indicates Congress intended to exclude subject matter from the FDA's jurisdiction in an "extraordinary case" in which the "unique political history" suggested that Congress was unlikely to have delegated authority to the agency in such a "cryptic" fashion).

[60] Michigan v. EPA, 576 U.S. 743, 759 (2015) ("The Agency must consider cost—including, most importantly, cost of compliance—before deciding whether regulation is appropriate and necessary.").

[61] 42 U.S.C. § 1395x(v)(1)(A).

[62] *See, e.g.*, Villa View Cmty. Hosp., Inc. v. Heckler, 728 F.2d 539, 540 (D.C. Cir. 1984) ("Congress has given the Secretary considerable discretion to promulgate cost-reimbursement regulations that give meaning to the term 'reasonable costs.'"); John L. Doyne Hosp. v. Johnson, 603 F. Supp. 2d 172, 180 (D.D.C. 2009) (recognizing "the ambiguity inherent in [reasonable cost] and the broad delegation of authority to issue regulations developing the 'reasonable cost' concept"); Sid Peterson Mem'l Hosp. v. Thompson, 274 F.3d 301, 307 (5th Cir. 2001) ("We are not empowered to overrule the Secretary's interpretation merely because it does not coincide with our own notion of 'reasonable cost' . . . ."). In each of these cases, the court reached the second *Chevron* step after concluding that "reasonable cost" was ambiguous.

which any FDA construction would receive deference. "Safety" and "effectiveness" can likewise be read as ambiguous. Safety and effectiveness are always relative, since no device is completely safe, and effectiveness can never be one hundred percent. FDA will receive deference for any reasonable interpretation, and it is reasonable to consider costs in the innately relative requirements on safety and effectiveness.

Moreover, other agencies have successfully interpreted silence about economic costs as allowing them to consider such costs in their cost-benefit analyses. The Federal Trade Commission Act, the FTC's authorizing statute, simply empowers the FTC to prevent and penalize unfair and deceptive practices.[63] Yet the FTC conducts cost-benefit analyses in determining whether practices are unfair.[64] The FTC derives this implicit test from the statutory directive that conduct is unfair only if "not outweighed by countervailing benefits to consumers or to competition."[65] Although the statute merely specifies "benefits" rather than any mention of financial costs, the FTC interprets benefits to include decreased cost of a product, since the decreased cost is a benefit to consumers.[66] The FTC thus has authorization to consider economic costs when evaluating whether practices are unfair.

FDA can pursue a similar argument. Just as the FTC's authorizing statute makes no mention of economic costs faced by regulated parties, so too is FDA's authorizing statute silent

---

[63] 15 U.S.C. § 45.

[64] Maureen K. Ohlhausen, *Weigh the Label, Not the Tractor: What Goes on the Scale in an FTC Unfairness Cost-Benefit Analysis?* 83 GEO. WASH. L. REV. 1999, 2001 (2015) ("One of the foundations for the agency's successful use of this authority is the three-part test for unfairness, which includes a de facto cost-benefit analysis. To invoke unfairness successfully, the Commission must show that the conduct at issue causes or is likely to cause substantial harm to a consumer, that the consumer cannot reasonably avoid that harm, and the harm is not outweighed by the conduct's benefits to consumers or competition.").

[65] 15 U.S.C. § 45(n). This implicit test is conducted as part of a three-prong unfairness test, which evaluates (1) whether the practice offended public policy; (2) whether the practice was unethical, immoral, oppressive, or unscrupulous; and (3) whether it caused substantial injury to consumers or competitors. Ohlhausen, *supra* note 64, at 2001.

[66] *See* Ohlhausen, *supra* note 64, at 2019 (describing how the FTC considers cost savings from an entity's failure to take a precaution as a benefit to be weighed against the cost of harm to consumers).

on the issue. If the FTC can nonetheless consider costs, so too can FDA. Arguably, the standard of "reasonable assurance" applies a threshold of enforcement that FDA must minimally adopt, a threshold that is not specified for the FTC. Still, economic costs make sense as a part of cost-benefit analyses for both agencies. Lower costs of products are a benefit to both consumers protected by the FTC and patients protected by FDA. Thus, FDA can consider the economic cost of devices as part of its cost-benefit analysis.

C. Current Practices

Although FDA has disavowed considering economic costs as an explicit factor in approving medical devices,[67] in practice the agency has come up with limited and nuanced ways to consider costs, reflecting an underlying understanding that costs are an important consideration. Specifically, FDA considers costs in four ways: (1) consideration of non-financial costs in deciding whether to approve a product, (2) consideration of financial costs in deciding the speed of review, (3) consideration of financial impacts of major regulations and reporting requirements, and (4) implicit consideration of financial costs in decisions to approve products. All these practices represent exceptions to FDA's practice of disregarding costs, indicating that the agency recognizes the importance of considering costs and does not see the FDCA as a categorical prohibition on cost considerations.

1. Non-Financial Costs

FDA differentiates between financial and non-financial costs, believing that its statutory prohibition applies only to financial costs. This is supported by *Riegel*, where the Supreme Court

[67] *See supra* notes 8, 37-40 and accompanying text.

favorably noted that FDA conducts cost-benefit analysis by balancing risks and benefits.[68] But in describing the cost-benefit analyses that FDA conducts, the Court described only costs to health, such as the potential for patient harm, not economic costs.[69] Still, the Court has never explicitly drawn a distinction between economic and health costs when interpreting the FDCA's reasonable assurance standard. Thus, FDA's differentiation between financial and non-financial costs is not precluded by case law.

2. Speed of Review

Interestingly, the FDCA implicitly condones the use of cost-benefit considerations when determining the timing of review. The sections of the FDCA authorizing expedited review do not make any mention of economic costs.[70] Instead, the FDCA simply specifies other criteria for expedited review, such as whether a drug intends to "treat a serious or life-threatening disease or condition."[71] Implicitly, however, when deciding which drugs to expedite, FDA necessarily considers the impact of accelerated approval on decreasing hospitalization and other costs.[72]

In addition, despite having no clear statutory authorization to do so, FDA officials have openly discussed how financial costs create the need for speedier review.[73] For example, FDA Commissioner Scott Gottlieb wrote on an FDA blogpost that "[w]e could see even greater cost

[68] 552 U.S. at 325 ("A state statute, or a regulation adopted by a state agency, could at least be expected to apply cost-benefit analysis similar to that applied by the experts at the FDA: How many more lives will be saved by a device which, along with its greater effectiveness, brings a greater risk of harm?").
[69] *Id.*
[70] 21 U.S.C. § 356(a)(1).
[71] *Id.*
[72] OFF. OF TECH. ASSESSMENT *supra* note 35, at 89.
[73] Scott Gottlieb, *FDA Working to Lift Barriers to Generic Drug Competition*, FOOD & DRUG ADMIN. (June 21, 2017), https://www.fda.gov/news-events/fda-voices/fda-working-lift-barriers-generic-drug-competition.

savings if we helped more safe and effective generic drugs get to market sooner," discussing a new regulatory plan that aimed to speed generic drug approvals.[74]

Since the FDCA makes no mention of cost considerations in speed of review, FDA is simply filling a gap where the statute is silent. The agency should likewise be able to fill the statutory gap on cost considerations in approval decisions. If FDA can prioritize faster approval of low-cost drugs, it can also weigh costs when evaluating the safety and effectiveness of products.

3. Economic Impact Analyses of Proposed Regulations

FDA does not issue regulations when assessing the safety and effectiveness of products, since approving a specific device constitutes adjudication. When the agency issues major regulations, however, it must conduct economic impact analyses, which include "an assessment of the costs, benefits, and cost-effectiveness of the action, as well as assessments of the costs, benefits and cost-effectiveness of the most promising alternative actions."[75] Federal statutes and executive orders require all agencies, including FDA, to conduct economic impact analyses of important regulations.[76] FDA's economic impact analyses often focus on the costs of industry having to read and understand a final rule.[77] The analyses also consider how a regulation would increase the cost of medical products or disrupt health care delivery.[78]

---

[74] *Id.*
[75] *Economic Impact Analyses of FDA Regulations*, FOOD & DRUG ADMIN. (Feb. 4, 2022), https://www.fda.gov/about-fda/reports/economic-impact-analyses-fda-regulations.
[76] *See* 2 U.S.C. § 1532(a)(2); 5 U.S.C. §§ 601-612; Exec. Order No. 12866, § 6(a)(3)(C), 3 C.F.R. 638, _ (1993); Exec. Order No. 13563, § 1(b), 3 C.F.R. 215, _ (2012).
[77] FOOD & DRUG ADMIN., MEDICAL DEVICE DE NOVO CLASSIFICATION PROCESS: FINAL RULE 4-5 (2021), https://www.fda.gov/media/152744/download.
[78] OFF. OF TECH. ASSESSMENT, *supra* note 35, at 91-92 (illustrating "FDA's use of cost-benefit analysis to evaluate one of its regulations" when the agency recognized that its regulation would increase the cost of X-ray equipment and disrupt health care delivery).

The FDCA also requires FDA to consider the economic impact of reporting requirements imposed on industry actors.[79] FDA can require manufacturers only to provide information according to the "least burdensome" standard, limited to "the minimum amount of information necessary to adequately address a relevant regulatory question or issue through the most efficient manner at the right time."[80]

Although not explicitly required to do so, FDA could adopt similar approaches to considering costs related to its adjudications.

4. Implicit Consideration in Product Approval Decisions

Implicitly, a variety of FDA decisions may reflect consideration of economic costs in the approval stage despite the agency's belief that the statute prohibits such consideration.[81] In our conversations with FDA reviewers, we learned that reviewers will not explicitly name cost as a consideration but may come up with proxy considerations to justify a decision influenced by cost.[82] For example, if a new medical device is substantially less expensive than existing alternatives, the reviewer who wants to approve the product might instead cite the fact that the device is smaller than alternatives and thus takes up less space in a health care facility.[83] This backdoor path for cost considerations reflects that FDA reviewers understand that a realistic approach to product approval must incorporate costs.

---

[79] 21 U.S.C. § 360c(a)(3)(D)(ii), (c)(5)(A), (i)(1)(D)(i); FOOD & DRUG ADMIN., THE LEAST BURDENSOME PROVISIONS: CONCEPT AND PRINCIPLES(Feb. 5, 2019), https://www.fda.gov/media/73188/download.
[80] *The Least Burdensome Provisions: Concept and Principles*, *supra* note 79.
[81] *See, e.g.*, OFF. OF TECH. ASSESSMENT, *supra* note 35, at 88-92 (explaining several scenarios in which costs are an implicit factor in FDA decision-making); Cooper, *supra* note 38, at 801 ("When I was at the agency, discretionary application of economic considerations was unproblematic; and I believe it still is.").
[82] Interview with FDA Reviewer (Aug. 2021) (notes on file with authors).
[83] *Id.*

D. General Guidance on Software

As was the case with drugs and devices,[84] FDA's scrutiny of software arose out of tragedy when the Therac-25, the first radiation machine controlled primarily by software, overradiated six patients in the United States and Canada between 1985 and 1987, causing serious injuries and three deaths.[85] FDA responded by issuing a draft document in 1987 commonly known as the "Draft Software Policy," which attempted to formulate a general policy toward software that varied the level of oversight depending on the risk to the patient.[86]

FDA attempted to push this process forward, revising the Draft Software Policy in 1989[87] and holding public workshops on further proposed changes.[88] It also included some discussion in its 1996 Quality System Regulation, which underscored the importance of augmenting inspection and testing of software with properly validated quality and design control systems.[89] As a result, it included "software validation and risk analysis" as part of required procedures for validating device design.[90]

---

[84] *See supra* notes 34-36 and accompanying text.
[85] For a comprehensive account of these incidents, see Nancy Leveson & Clark Turner, *An Investigation of the Therac-25 Accidents*, 26 IEEE COMPUT. 18 (1993).
[86] FDA Draft Policy Guidance for the Regulation of Computer Products, 52 Fed. Reg. 36,104 (Sept. 25, 1987).
[87] FOOD & DRUG ADMIN., DRAFT POLICY FOR THE REGULATION OF COMPUTER PRODUCTS (Nov. 13, 1989), *available at* 1989 WL 1178702 (revising the Draft Software Policy).
[88] *See* Medical Devices; Medical Software Devices; Notice of Public Workshop, 61 Fed. Reg. 36,886 (July 15, 1996) (announcing joint FDA-National Library of Medicine public workshop on medical software devices to be held on September 3-4, 1996); E. Stewart Crumpler & Harvey Rudolph, *FDA Software Policy and Regulation of Medical Device Software*, 52 FOOD & DRUG L.J. 511, 514-16 (1997) (describing the public workshop described above as well as another workshop in 1996 designed to obtain public feedback on its proposed revisions); Fried & Zuckerman, *supra* note 9, at 130, 133-36 (describing the second 1996 workshop and FDA's intent to issue new guidelines in late 2020).
[89] Medical Devices; Current Good Manufacturing Practice ("CGMP"), 61 Fed. Reg. 52,602, 52,606 ¶ 7, 52,617 ¶ 68, 52,630 ¶ 136 (Oct. 7, 1996).
[90] 21 C.F.R. § 820.30(g).

Despite these efforts, FDA abandoned the effort in 2005.[91] Although FDA simply included the Draft Software Policy in a list of withdrawn guidance without offering any further comment, later pronouncements made clear that the agency had come to believe that software was too complex and fast moving to be governed by a single overarching policy.[92] Instead of making rules, FDA began classifying different types of software as Class I, II, or III devices on a case-by-case basis that provided little guidance for future decisions.[93] FDA supplemented these adjudications with nonbinding guidance documents on a number of various software-related topics.[94]

Commentators have criticized the ad hoc nature of FDA's approach for its failure to provide clear guidance to regulated entities.[95] Congress has also appeared to recognize FDA's

---

[91] Annual Comprehensive List of Guidance Documents at the Food and Drug Administration, 70 Fed. Reg. 824, 890 (Jan. 5, 2005).

[92] *See, e.g.*, Devices: General Hospital and Personal Use Devices; Reclassification of Medical Device Data Systems, 73 Fed. Reg. 7,498, 7,499 (Feb. 8, 2008) (proposed rule) (concluding that increase in the number and complexity of software-based medical devices "have created new considerations for elements of risk that did not previously exist" And that "[b]ased on this history and the complexity and diversity of computer software, FDA decided it would be impractical to prepare one 'software' or 'computer' policy that would be able to address all the issues related to the regulation of computer- and software-based medical devices"); Medical Devices; Medical Device Data Systems, 76 Fed. Reg. 8,637, 8,638 (Feb. 15, 2011) (final rule) (concluding that "because of the history, complexity, and diversity of computer systems and controlling software, it would be impractical to adopt one 'software' or 'computer' policy to address all computer and software medical devices"); FOOD & DRUG ADMIN., DRAFT GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF: MOBILE MEDICAL APPLICATIONS 5 (July 21, 2011), *available at* https://appletoolbox.com/wp-content/uploads/2014/03/ UCM263366.pdf, *notice provided at* 76 Fed. Reg. 43,689 (July, 21, 2011) (concluding that "it would be impractical to prepare an overarching software policy to address all of the issues related to the regulation of all medical devices containing software" because "the use of computer and software products as medical devices grew exponentially and the types of products diversified and became more complex"); 2019 FDA SOFTWARE FUNCTIONS GUIDANCE, *supra* note 19, at 34.

[93] Nathan Cortez, *Regulating Disruptive Innovation*, 29 BERKELEY TECH. L.J. 175, 193 (2014); W. Nicholson Price II, *Regulating Black-Box Medicine*, 116 MICH. L. REV. 421, 443 (2017); Scott D. Danzis & Christopher Pruitt, *Rethinking the FDA's Regulation of Mobile Medical Apps*, ABA SCITECH LWYR., Winter/Spring 2013, at 26, 27. These ad hoc categories include "medical calculators, cameras, lights, magnifiers, microscopes, monitors, recorders, reminders, scales, surgical tools, transmitters, and a host of data systems that store, display, and manipulate information." Nathan Cortez, *The Mobile Health Revolution?*, 47 U.C. DAVIS L. REV. 1173, 1221 (2013).

[94] *See, e.g.*, General Principles of Software Validation; Final Guidance for Industry and FDA Staff, 67 Fed. Reg. 1,482 (Jan. 11, 2002); FOOD & DRUG ADMIN., GUIDANCE FOR THE CONTENT OF PREMARKET SUBMISSIONS FOR SOFTWARE CONTAINED IN MEDICAL DEVICES 4-10 (May 11, 2005), https://www.fda.gov/media/73065/ download [hereinafter 2005 FDA PREMARKET SOFTWARE GUIDANCE]; 2019 FDA SOFTWARE FUNCTIONS GUIDANCE, *supra* note 19.

[95] *See, e.g.*, Cortez, *supra* note 93, at 193; Price, *supra* note 93, at 443.

shortcomings. For example, in 2016, Congress passed the 21st Century Cures Act, which specified that medical devices regulated by FDA excludes software functions intended for administrative support, maintaining or encouraging a healthy lifestyle, electronic patient records, or handling clinical laboratory test results.[96] Legislative exemptions of specific technologies are likely to be proven as unpredictable as ad hoc regulatory decisions.

Hidden in these guidance documents is a subtle shift toward greater openness to cost-benefit analysis. FDA's 2005 Guidance for the Content of Premarket Submissions for Software Contained in Devices followed the established path of focusing only on health-related concerns when it based the level of recommended documentation based on the likelihood that product failure could lead to injury or death for the patient or operator.[97] The 2021 proposed revisions to this guidance continue to focus on health-related concerns, keying the required level of documentation on whether "[a] failure or latent flaw of the device software function(s) could present a probable risk of death or serious injury" to patients, users, or others in the environment of use.[98] At the same time, the 2021 draft guidance creates more room for benefit-risk analysis in its recommendation that software manufacturers assess risk, as well as the acceptability of residual risk, in developing risk management plans.[99] When residual risks are not considered acceptable according to a manufacturer's risk management plan, the manufacturer should "provide documented evidence to demonstrate that the benefits of the intended use outweigh the residual risk." [100] FDA does not define how to determine the "acceptability" of a risk. Instead, the

---

[96] Pub. L. No. 114-255, § 3060, 130 Stat. 1033, 1130 (2016) (codified at 21 U.S.C. § 360j(o)(1)(A)-(D)).
[97] 2005 FDA PREMARKET SOFTWARE GUIDANCE, *supra* note 94, at 4-10.
[98] FOOD & DRUG ADMIN., CONTENT OF PREMARKET SUBMISSIONS FOR DEVICE SOFTWARE FUNCTIONS: DRAFT GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 7-8, 17 (Nov. 4, 2021), https://www.fda.gov/media/153781/download. This draft guidance was intended to supersede earlier FDA guidance issued in 2005. *Id.* at [title page].
[99] . *Id.* at 9, 15-18.
[100] *Id.* at 17.

guidance instructs manufacturers to develop their own risk acceptability criteria and then conduct risk-benefit analyses of any residual risks that do not meet the acceptability criteria.[101]

E. Specific Guidance on Cybersecurity Management

As part of its suite of guidance documents on software, FDA has issued specific guidance on the management of cybersecurity. Specifically, FDA issued guidance in 2014 regarding premarket submissions for management of cybersecurity in medical devices.[102] It followed that up in 2016 with guidance regarding postmarket management of cybersecurity of those same devices.[103] It also released revised draft guidelines on premarket submissions for cybersecurity in 2018.[104] FDA regards cybersecurity management as part of the software validation and risk analysis required by the Quality System Regulation.[105]

At first glance, these guidance documents appear to adhere to FDA's practice of considering only health-related risks and benefits and to disregard economic costs and benefits. For example, the 2014 premarket cybersecurity guidance called on manufacturers to take a risk-based approach, where risk is defined in terms of harm as measured by "physical injury or damage to the health of people, or damage to property or the environment."[106] Similarly, the

---

[101] *Id.* at 15, 17.
[102] FOOD & DRUG ADMIN., CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 4 (Oct. 2, 2014), https://www.fda.gov/media/86174/download [hereinafter 2014 FDA PREMARKET CYBERSECURITY GUIDANCE].
[103] FOOD & DRUG ADMIN., POSTMARKET MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 9 (Dec. 28, 2016), https://www.fda.gov/media/95862/download [hereinafter 2016 FDA POSTMARKET CYBERSECURITY GUIDANCE].
[104] FOOD & DRUG ADMIN., CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: DRAFT GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 8 (Oct. 18, 2018), https://www.fda.gov/media/119933/download [hereinafter 2018 FDA PREMARKET CYBERSECURITY DRAFT GUIDANCE]. This draft guidance explicitly indicates that it is intended to supersede the guidance FDA issued in 2014. *Id.* at tit.
[105] 2014 FDA PREMARKET CYBERSECURITY GUIDANCE, *supra* note 102, at 4 (citing 21 C.F.R. 820.30(g)); 2016 FDA POSTMARKET CYBERSECURITY GUIDANCE, *supra* note 103, at 13 (same); 2018 FDA PREMARKET CYBERSECURITY DRAFT GUIDANCE, *supra* note 104, at 8 (same).
[106] 2014 FDA PREMARKET CYBERSECURITY GUIDANCE, *supra* note 102, at 3, 4.

2014 guidance's endorsement of the National Institute of Standards and Technology's framework of five core cybersecurity functions that every manufacturer should perform focused on "the probable risk of *patient harm* due to a cybersecurity breach."[107] It also recommends that manufacturers strike a balance between cybersecurity safeguards and the usability of the device," such as by ensuring that "security controls [do] not unreasonably hinder access to a device intended to be used during an emergency situation."[108]

The 2016 postmarket cybersecurity guidance bore similar signs. First, it repeatedly framed the issue in terms of "patient harm,"[109] which it defined as "physical injury or damage to the health of patients, including death."[110] The discussion of risk management was similarly framed in terms of patient harm.[111] In particular, the core recommendations on risk management focus on "assessing the severity of patient harm" and "evaluat[ing] . . . the risk of patient harm."[112]

The 2018 proposed revisions to the 2014 premarket cybersecurity guidance reflect the same approach, framing its recommendations largely in terms of patient harm.[113] Similar to the 2014 guidance, the 2018 draft also defines patient harm as "physical injury or damage" to patient health.[114] It extends it by recommending that manufacturers "promote the development of trustworthy devices," where trustworthiness is again largely framed in terms of patient harm.[115]

---

[107] *Id.* at 4 (emphasis added) (citing NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL CYBERSECURITY (Feb. 12, 2014), *available at* https://nvlpubs.nist.gov/nistpubs/cswp/ nist.cswp.02122014.pdf).
[108] *Id.* at 4.
[109] 2016 FDA POSTMARKET CYBERSECURITY GUIDANCE, *supra* note 103, at 5, 6, 9, 11, 13-15.
[110] *Id.* at 10.
[111] *Id.* at 15.
[112] *Id.* at 17.
[113] 2018 FDA PREMARKET CYBERSECURITY DRAFT GUIDANCE, *supra* note 104, at 4, 5, 10, 12.
[114] *Id.* at 8.
[115] *Id.* at 9, 12, 16.

But lurking in these cybersecurity guidance documents' discussions of risk are tantalizing hints of increased willingness to take economic costs and benefits into account. For example, the 2014 premarket guidance's emphasis on usability provides an angle for taking cost considerations into account indirectly.[116] More explicitly, calling for an "[a]ssessment of residual risk and risk acceptance criteria" acknowledges that complete remediation of cybersecurity risk is not always possible.[117] The 2014 premarket guidance provides no basis for determining what types of risks are acceptable. The 2014 premarket guidance further recommends that manufacturers provide justifications for the security features they choose to incorporate but again provides no further details on what would constitute a valid justification.[118]

FDA's 2016 postmarket cybersecurity guidance provides further hints at cost-benefit balancing when it reiterates the recommendation in the 2014 premarket cybersecurity guidance that manufacturers undertake "assessment[s] of residual risk and risk acceptance criteria."[119] After defining cybersecurity risk in terms of exploitability and severity of patient harm, the guidance states that a "[c]ontrolled risk is present when there is sufficiently low (acceptable) residual risk of patient harm," whereas "[u]ncontrolled risk is present when there is unacceptable residual risk of patient harm due to inadequate compensating controls and risk mitigation."[120] The 2016 postmarket guidance recommends a series of changes and compensating actions that help address both types of risks and lays out examples of both controlled and uncontrolled risks and their management.[121]

---

[116] *See supra* note 83 and accompanying text
[117] 2014 FDA PREMARKET CYBERSECURITY GUIDANCE, *supra* note 102, at 4.
[118] *Id.*
[119] 2016 FDA POSTMARKET CYBERSECURITY GUIDANCE, *supra* note 103, at 9.
[120] *Id.* at 9, 12.
[121] *Id.* at 19-24.

The 2018 draft premarket cybersecurity guidance follows the lead of the earlier guidance in calling for an "assessment[s] of residual risk and risk acceptance criteria," again without defining what those criteria might be.[122] It adds another level to the analysis by using risk levels to divide devices into two tiers, with higher levels of documentation required of devices posing greater cybersecurity risks to patients.[123] The 2018 draft guidance also recommends that manufacturers design devices that are "trustworthy," with the requirements varying by tier of cybersecurity risk.[124] According to the draft guidance, trustworthy devices "(1) are reasonably secure from cybersecurity intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures."[125]

In terms of cybersecurity, the 2014 and 2016 guidelines and the 2018 draft guidelines all recognize the need to tolerate an acceptable level of residual risk. Although none specifies how that level should be set, together they implicitly acknowledge that some risks cannot be addressed without undue costs. Furthermore, the repeated references to reasonableness in the 2018 draft guidance also seem to invite consideration of costs.

In any event, existing practices permit FDA to take economic costs and benefits into account indirectly when determining the appropriate level of cybersecurity. For example, given that any increase in cybersecurity requirements necessarily would require additional processing or storage and would affect battery life, FDA can fit economic considerations into its practice of

---

[122] 2018 FDA PREMARKET CYBERSECURITY DRAFT GUIDANCE, *supra* note 104, at 9
[123] *Id.* at 11, 21.
[124] *Id.* at 11.
[125] *Id.* at 8.

considering whether additional measures to improve safety or effectiveness might increase the size of the device.[126]

III. Approaches to Determining the Optimal Level of Cybersecurity

The foregoing analysis suggests that FDA possesses the legal authority to take economic costs into account when assessing medical devices in general and software in particular. This Section addresses whether FDA should exercise that authority and, if so, how.

A. The Case of Cybersecurity

The need to balance economic costs and benefits looms particularly large for cybersecurity. As an initial matter, minimizing the potential health dangers that would result if a medical device were hacked should be an inherent part of FDA's statutory obligation to provide a reasonable assurance of safety. However, like other software issues, cybersecurity was not the intended object of the regulatory scheme devised for FDA decades ago. The result is a jarring mismatch between FDA's approach to regulation and the unique needs of software and cybersecurity.

Furthermore, cybersecurity harm cannot be reduced to a statistical probability, making perfect cybersecurity impossible. As noted earlier, no matter how much manufacturers spends on cybersecurity, their devices will never be 100% secure. Designers cannot predict the innovations of malicious actors, and the unbounded nature of physical inputs mean unbounded risks. In cybersecurity, a notion of acceptable risk is inevitable. As a result, a "reasonable assurance of

[126] *See supra* note 83 and accompanying text.

safety and effectiveness" in the context of cybersecurity cannot be accomplished without some type of cost-benefit analysis.

B. Possible Approaches to Taking Economic Cost into Account

Although FDA would be taking an important step in construing the FDCA as permitting consideration of costs in medical device cybersecurity, doing so would still leave many questions unresolved. Simply put, many approaches exist to taking costs into consideration. In this part, we consider three approaches: the FTC's cost-benefit test, the risk-utility calculus from tort law, and Incremental Cost Effectiveness Ratios ("ICERs") that have become increasingly popular in some health care circles.

1. The FTC's Cost-Benefit Test

As discussed in Part II, the FTC uses a de facto cost-benefit analysis to assess whether conduct is unfair.[127] The test assesses whether the injury caused by a particular practice outweighs the benefits of that practice.[128] Benefits include economic costs, since lower costs create a benefit to consumers.

FDA could adopt the FTC's de facto cost-benefit analysis. In this case, FDA would assess each decision by a designer to include or omit a cybersecurity feature, asking whether the harm is outweighed by the benefits of that decision. The cost savings from omitting a feature would factor into the benefits, as would any positive impact on functionality. Thus, this cost-benefit analysis would require designers to show that the benefits—the reduced cost and

---

[127] *See supra* notes 64-66 and accompanying text.
[128] Ohlhausen, *supra* note 64, at 2012.

increased functionality—associated with omitting a cybersecurity feature exceed the increased risk of cybersecurity harm.

Just as the FTC has discretion in enforcing unfair and deceptive practices, this approach would provide discretion to FDA in evaluating cybersecurity practices. Discretionary enforcement could be used to target offenders in a way that balances security precautions with promoting innovation.[129]

This approach provides a clear cost-benefit test while emphasizing flexibility because of the discretion available to the enforcing agency. Furthermore, the approach has strong legal justification since the FTC's authorizing statute matches FDA's in its statutory silence on the consideration of financial costs.[130]

2. Tort Standards

Tort law has, over the years, involved a variety of standards for product liability. At one point, many courts applied strict liability, imposing liability regardless of the seller's fault.[131] But pushback occurred as observers noted that "[n]o one wants absolute liability where all the article has to do is cause injury."[132] Since then, courts, legislatures, and regulators have sought to reform product liability standards. Today, states primarily apply one of two tests, or some combination of the two, for product liability: the consumer expectations test and the risk utility

[129] Derek E. Bambauer, *Cybersecurity for Idiots*, 106 MINN. L. REV. HEADNOTES 172, 192-93.
[130] *See supra* Part II.B.
[131] DAVID G. OWEN, PRODUCTS LIABILITY LAW 298-300 (3d ed. 2015) (describing the strict liability standard and the gradual shift to consumer expectations and risk utility tests).
[132] *Id.* at 299.

test.[133] Although most states have yet to fully adopt the Third Restatement's approach to product liability, the risk utility test has become the dominant standard for design defects.[134]

These tests have resulted from different iterations of the Restatement of Torts as policymakers debated how far the optimal standard should depart from strict liability. The Second Restatement of Torts established the consumer expectations test.[135] It asks whether a product is defective because the product is "more dangerous than an ordinary consumer would expect when used as intended or in a reasonably foreseeable manner."[136]

Some states apply a consumer expectations test to tort liability claims for medical devices.[137] This test, however, turned out to pose multiple problems in practice.[138] Critics, for example, have noted that it can reward designers who fail to adopt cost-effective measures that could solve obvious threats to safety.[139] Furthermore, the consumer expectations test is ill suited for complex medical devices that do not parallel normal consumer products purchased at a store.[140] A Florida court held that "the consumer expectations test cannot be logically applied here, where the product in question is a complex medical device available to an ordinary

---

[133] *Id.* at 504 ("Although most modern courts have abandoned consumer expectations as the predominant test for design defectiveness, . . . some courts still use this test in design defect cases."); *id.* at 507 n. 34 (noting examples of laws in Tennessee, Ohio, and Washington that blend the consumer expectations and risk-utility tests).
[134] *Id.* at 508-09.
[135] *Id.* at 301.
[136] RESTATEMENT (SECOND) OF TORTS § 402A (AM. L. INST. 1965).
[137] *See, e.g.*, Miller v. DePuy Synthes Sales, Inc., 837 F. Appx. 472, 473-74 (9th Cir. 2020); Cavanaugh v. Stryker Corp., 308 So. 3d 149, 153 (Fla. Dist. Ct. App. 2020).
[138] OWEN, *supra* note 131, at 305-09 (discussing the practical problems that arise when courts try to implement the consumer expectations test).
[139] *Id.* at 506 ("[A] dire consequence of the consumer expectations test, unless its plain consequences are baldly ignored, is that it effectively rewards manufacturers for failing to adopt cost-effective measures to remedy obviously unnecessary dangers to human life and limb. The failure of the consumer expectations test to deal adequately with the obvious danger problem profoundly weakens the usefulness of this test and effectively disqualifies it for principled use as the sole basis for determining defects in design.").
[140] Eric Alexander, *Design Claims Fail Under Consumer Expectations Test with an Adequate Warning*, DRUG & DEVICE LAW (Jan. 15, 2021), https://www.druganddevicelawblog.com/2021/01/design-claims-fail-under-consumer-expectations-test-with-an-adequate-warning.html; *see also* OWEN, *supra* note 131, at 507 (noting "the vagueness of a consumer's expectations concerning most complex designs").

consumer only as an incident to a medical procedure. After all, medical device manufacturers generally do not market their products to 'ordinary consumers.'"[141] In practice, the consumer expectations test is so complex that even when courts officially use the consumer expectations test, they actually apply some form of cost-benefit analysis to determine design defects.[142]

In response, the Third Restatement represented a full shift away from strict liability and toward the standard of negligence by replacing the consumer expectations test with the risk utility test.[143] This test requires the plaintiff to demonstrate the existence of a reasonable alternative design.[144] Under the risk utility test, a "product is unreasonably dangerous if the risk of danger in the design outweighs the benefit."[145] Courts "saw the wisdom of assessing design defectiveness according to whether the safety benefits of remedying a design danger were worth the costs."[146]

This analysis, by itself, resembles the standard currently applied by FDA, which evaluates whether safety risks outweigh the benefits of a product's effectiveness. But the reasonable alternative design requirement adds another layer that FDA could adopt. Under the reasonable alternative design requirement, courts assess "whether a reasonable alternative design would, at a reasonable cost, have reduced the foreseeable risk of harm posed by the product and, if so, whether the omission of the alternative design by the seller . . . rendered the product not reasonably safe."[147] This is somewhat analogous to the Hand Test, which requires cost-justified

---

[141] *Cavanaugh*, 308 So. 3d at 155.

[142] *See* OWEN, *supra* note 131, at 507 ("Some courts that use the consumer expectations test limit the applicability of the test to cases involving simple, rather than complex, product designs and accident mechanisms. . . . Some courts and legislatures are more generally blending the consumer expectations test with the risk-utility standard . . ..").
[143] *Id.* at 309-13 (discussing the decline of the consumer expectations test and the shift to the risk-utility test).
[144] RESTATEMENT (THIRD) OF TORTS: PRODUCT LIABILITY § 2(b) (AM. L. INST. 1997); *see also, e.g.*, Cavanaugh, 308 So. 3d at 153.
[145] *Cavanaugh*, 308 So. 3d at 153.
[146] OWEN, *supra* note 131, at 508.
[147] RESTATEMENT (THIRD) OF TORTS, *supra* note 144, § 2 cmt. d.

precautions where marginal benefit exceeds marginal cost.[148] The "reasonable cost" requirement, if adopted by FDA, would enable the agency to require only a standard of safety that is justified by costs.

Given the impractical application of the consumer expectations test to medical device cybersecurity, only the risk utility test would make sense as an option for FDA. This approach would be one already familiar to designers, but it leaves unclear the specific level of risk that is "reasonable." Although preemption of state tort law by FDA is a contested issue,[149] we need not address this issue here. If tort law is preempted, FDA would simply adopt versions of the tort standards as regulatory standards. Although adopting tort standards that have been preempted carries some irony, embodiment in federal law would provide a uniform standard that would replace the myriad approaches taken by different states.

That said, the alternative design approach makes a poor fit with software. This is because the standard approach of comparing the cost of the alternative design with its benefit is inapt for products such as software, where differences in the cost of the actual products are negligible and the real differences lie in development costs.

3. Incremental Cost Effectiveness Ratios ("ICERs")

Health economists commonly use Incremental Cost Effectiveness Ratios ("ICERs") to measure cost effectiveness,[150] and FDA could adopt this framework to determine the optimal

---

[148] United States v. Carroll Towing, 159 F.2d 169, 173 (2d Cir. 1947).
[149] *See, e.g.*, Marcia Boumil, *FDA Approval of Drugs and Devices: Preemption of State Laws for "Parallel" Tort Claims*, 18 J. HEALTH CARE L. & POL'Y 1 (2015).
[150] PETER MUENNIG & MARK BOUNTHAVONG, COST-EFFECTIVENESS ANALYSIS IN HEALTH 9-10 (3d ed. 2001) (discussing the primary use of ICER in comparing pharmaceuticals and other medical products).

level of risk. Under this approach, FDA would set a clear standard requiring any cybersecurity improvement that is cost-effective.

An ICER compares the marginal cost of a proposed intervention to its marginal effectiveness.[151] The lower the value of an ICER, the more cost-effective an intervention. If an ICER for an intervention is lower than a predefined threshold of cost-effectiveness, then the intervention is considered cost-effective.[152]

Using this approach, FDA would set a threshold ICER to delineate which cybersecurity features are cost effective. FDA would need to collect data on the costs and effectiveness of cybersecurity features to establish the ICER for each possible security feature. Designers would then be responsible for including any cybersecurity intervention that falls within that threshold. As part of this standard, designers would need to account for updates. If an update would be cost effective, it would be required.

A major challenge would be defining "effectiveness." Common metrics of effectiveness, such as Quality-Adjusted Life Years ("QALY"), Disability-Adjusted Life Years ("DALY"), and Value of a Statistical Life ("VSL"), pose multiple challenges. In general, these metrics can be controversial. They attempt to monetize the value of benefits by estimating the value of life, but such issues tend to be highly controversial.[153] For example, one scholar, arguing against the use

---

[151] *Id.* The equation is:

$$\text{ICER} = \frac{(\text{Cost of Alternative 2}) - (\text{Cost of Alternative 1})}{(\text{Effectiveness of Alternative 2}) - (\text{Effectiveness of Alternative 1})}$$

[152] As an example, the National Institute for Health and Care Excellence defines an intervention that costs less than £20,000 per QALY as cost effective. NAT'L INST. FOR HEALTH AND CARE EXCELLENCE, *The Guidelines Manual: Assessing Cost Effectiveness* (Nov. 30, 2012), https://www.nice.org.uk/process/pmg6/chapter/assessing-cost-effectiveness ("[I]n general, interventions with an ICER of less than £20,000 per QALY gained are considered to be cost effective.").

[153] W. Kip Viscusi, *The Value of Life*, *in* NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 586, 685 (2nd ed. 2008).

of QALYs in drugs reviews, criticized the QALY methodology for incorporating subjective values that are "at [their] root, random."[154] He further noted that reliance on the QALY could discourage research on rare diseases, which minimally improve societal QALYs.[155] More viscerally, the commentator derided the question of what a year of life is worth, saying, "[i]f I was asked that question about one of my children, my answer would be 'limitless,' and no one could persuade me otherwise. But others are putting a discrete price tag on it."[156]

Even accepting the usefulness of such metrics, these metrics are particularly complex to estimate in the context of cybersecurity.[157] Effectiveness would need to be defined by the estimated reduction in risk of harm related to cybersecurity. Change in risk of harm would be measured in terms of lives saved or improved. An intervention could be effective either by reducing the likelihood of a cybersecurity event or by mitigating the harm that such an event would have if it occurred. The baseline level of risk, too, would be difficult to estimate.[158] For future black swan events, probability and magnitude of harm may involve considerable speculation, especially for emerging technologies for which we have not had a chance to collect extensive data.

---

[154] William S. Smith, *The U.S. Shouldn't Use the 'QALY' in Drug Cost-Effectiveness Reviews*, STAT (Feb. 22, 2019), https://www.statnews.com/2019/02/22/qaly-drug-effectiveness-reviews/.
[155] *Id.*
[156] *Id.*
[157] Dan Geer, *For Good Measure: Security Measurement in the Present Tense*, USENIX, Fall 2020, at 72, 73, https://www.usenix.org/system/files/login/issues/login_fall20_issue.pdf ("Is something like DALY more like what we should be measuring in cybersecurity? Or is measurement of either the QALY and DALY sorts built on assumptions that don't actually obtain in cybersecurity? For that matter, where are the tails of distributions getting heavier—the prodromes of black swan events?").
[158] Alberto Galasso & Hong Luo, *Risk Perception, Tort Liability, and Emerging Technologies*, BROOKINGS (Mar. 23, 2021), https://www.brookings.edu/research/risk-perception-tort-liability-and-emerging-technologies/ ("[M]any risk factors—related to the ways in which humans interact with machines, the ways in which different components and different products interact with each other, and the ways in which consumers are harmed—may be difficult to predict ex-ante.").

Effectiveness should also take into account external benefits—benefits not directly affecting patients.[159] Such benefits may affect, for example, hospital systems or providers. External benefits, however, may be vague and difficult to quantify. Reliance on such measures could draw criticism that over-estimation of benefits leads to unduly burdensome requirements.[160]

Once effectiveness has been defined, regulators must decide on the threshold of cost-effectiveness. Doing so essentially requires putting a dollar amount on life. This can be determined, for example, using willingness-to-pay data measuring consumers' valuation of life, but the reliability and applicability of such data have been criticized.[161]

Once ICER calculations are complete, the standard would provide the clearest guidance for designers. However, this approach is the most granular and thus the most difficult to implement. Furthermore, FDA has been reluctant to rely on QALYs or DALYs in the past, reflecting a wariness of societal aversion to putting a price tag on life.[162]

C. Choosing the Best Approach

Ultimately, FDA needs to choose a method of balancing costs and benefits. The exact flavor of cost-benefit analysis is less important. But of the three options, we suggest that the

---

[159] *See* Iain Nash, *Cybersecurity in a Post-data Environment: Considerations on the Regulation of Code and the Role of Producer and Consumer Liability in Smart Devices*, 40 COMPUTER LAW & SEC. REV. (2021) (discussing cybersecurity risks posed to third parties).
[160] *See, e.g.*, 40 C.F.R. pt. 63 (discussing criticisms of considering "co-benefits" in EPA decision-making).
[161] Paul T. Menzel, *How Should Willingness-to-Pay Values of Quality-Adjusted Life-Years Be Updated and According to Whom?*, AMA J. ETHICS (2021), https://journalofethics.ama-assn.org/article/how-should-willingness-pay-values-quality-adjusted-life-years-be-updated-and-according-whom/2021-08.
[162] *See* Christopher M. Heimann et al., *Project: The Impact of Cost-Benefit Analysis on Federal Administrative Law*, 42 ADMIN. L. REV. 545, 622 (1990). FDA became more willing to rely on QALYs beginning in the early 1990s and accelerating the early 2000s. Matthew D. Adler, *QALYs and Policy Evaluation: A New Perspective*, 6 YALE J. HEALTH POL'Y L. & ETHICS 1, 4, 58 (2006). The agency appears to have confined its use of QALYs to balancing health benefits and costs. *Id.* at 59-60.

FTC's cost-benefit analysis is the best fit because it provides a clear test, enables agency discretion, and has the best statutory justification.

First, this approach defines a clear test: a cybersecurity feature must be included if its benefits outweigh its costs. Granted, calculating benefits and costs is not always straightforward. Nonetheless, these can be estimated. The analysis would provide a clearer standard than the risk utility test that ambiguously requires "reasonable cost." Although ICER calculations could also provide a clear test, FDA would save resources using the FTC approach because it need not calculate the costs and benefits of every potential cybersecurity feature for every medical device, as would be required by the ICER option.

Second, the FTC's cost-benefit approach permits FDA discretion in what to enforce. FDA can thus save resources by conducting analyses only when choosing to take enforcement action for a particular device. In addition, FDA can strategically employ its discretion to target offenders in a way that balances security precautions with promoting innovation. Additionally, unlike with the reasonable alternative test under tort law, the FTC approach does not require FDA to reject anything for which a reasonable alternative exists. Rather, FDA need simply require that the device's features provide greater benefit than harm, and doctors and patients will remain free to choose from multiple reasonable alternatives.

Third, the FTC's cost-benefit approach has the most defensible statutory basis. As discussed in Part II, the authorizing statutes for both the FTC and FDA make no mention of cost-benefit analysis or consideration of economic costs, yet the FTC has a well-established practice of applying these analyses. FDA's adoption of this practice should be analogously defensible.

Even if FDA prefers a different method of weighing costs and benefits, however, we make no strong objections. Good-faith arguments may exist for a variety of approaches. Most

important is that the agency use some manner of cost-benefit analysis to remedy the current inadequacies in cybersecurity regulation.

CONCLUSION

Until FDA steps up, cybersecurity standards for medical devices will remain problematically unclear. In this Essay, we explain the pressing need for defining an optimal level of cybersecurity in medical cyber-physical devices, for which perfect security is unfeasible. Some form of cost-benefit analysis is the logical solution to informing the right standard for security. We examine the statutory constraints on FDA's ability to conduct cost-benefit analyses, and we argue that FDA does have justification to consider economic costs in evaluating devices, especially in the context of cybersecurity. We then assess three approaches that FDA could adopt to weigh costs and benefits of cybersecurity features. We concluded that adoption of the FTC's implicit cost-benefit analysis would be most practical and statutorily justifiable.

But even if there is disagreement over which cost-benefit approach FDA should adopt, the critical point is that at least one approach should be adopted. FDA cannot go on ignoring economic costs and failing to set a clear standard for cybersecurity. The impossibility of eliminating cybersecurity risks, the unbounded possibilities of inputs for cyber-physical devices, and the indeterminable probability of deliberate cyberattacks make it impossible to determine optimal cybersecurity unless costs are weighed against benefits.

This Essay has been an exercise in the FDA-regulated medical device space. But cyber-physical systems exist across fields, from autonomous vehicles to smart grid sensors. The continuing expansion of cyber-physical systems and their unique cybersecurity concerns calls for a great deal of further research.