CLEVELAND STATE LAW REVIEW ET CETERA
VOLUME 68 JUNE 24, 2019 PAGES 1-13

# FROM FITBITS TO PACEMAKERS: PROTECTING CONSUMER PRIVACY AND SECURITY IN THE HEALTHTECH AGE

JUSTIN EVANS[1] & KATELYN RINGROSE[2]

ABSTRACT

As wearable and analytics technology continues to be aggressively adopted, there is a congruent rise in data collection from wearable healthtech devices. This unprecedented rise in data collection poses massive privacy and security issues. This note addresses the benefits of IoT healthcare wearables and implants, as well as identifies where the privacy and security of data accrued by such devices could be improved. In an effort to better encapsulate the issue surrounding wearable device data collection, the authors analyze the many benefits of wearable healthcare devices, as well as look into the false sense of trust consumers have in the privacy and security of their healthcare information. The authors discuss how consumer protections under current healthcare laws are lacking. In conclusion, they look to the future of wearable devices and how the data they generate and retain should be stored and protected in light of its sensitive nature.

[1] Justin Evans is a recent graduate from Michigan State University College of Law, who writes at the intersections of law, technology and health. Justin has his Master's in Cancer Biology from Vanderbilt University and a Bachelors in Chemistry from Fayetteville State University. Justin is an incoming intellectual property litigation associate at Goldberg Segalla.

[2] Katelyn Ringrose is a recent graduate from Notre Dame Law School, who writes on surveillance, privacy, and tech policy. Katelyn is the 2019-2021 Christopher Wolf Fellow at the Future of Privacy Forum in Washington, D.C.

## INTRODUCTION

The Internet of Things (IoT) is a network of computing devices comprised of a massive amount of everyday objects, sensors, and devices which send and receive data.[3] By 2020, there will be an estimated 31 billion devices connected to the internet, revolutionizing various industries, including healthcare.[4] Medical IoT devices are implanted and affixed to the human body to help with the early detection of diseases, manage pain, and encourage healthier lifestyles. Such devices are simultaneously generating a tremendous amount of data about patients' behaviors and physiologies. As more smart devices are incorporated into the healthcare industry, new concerns about their privacy and security arise.

Wearable technologies, like Fitbits and Apple Watches, have the capacity to track the location of a wearer, as well as his or her activity level, sleep patterns, heart rate and heart rate abnormalities, etc.[5] Such devices are paired with mobile applications and websites that link those pieces of information with a user's self-contributed information–including email addresses, phone numbers, height, weight, diet, etc. Internal healthcare devices, like pacemakers, are custom microprocessors similar to those used in mainframe computers.[6] Microprocessor-controlled pacemakers can record, process, and transmit information regarding a patient, pacemaker, and the interaction between them.[7]

This article will address the benefits of IoT healthcare wearables and implants, as well as identify where the privacy and security of data accrued by such devices could be improved. In Part I, we analyze the benefits of wearable healthcare devices, including the benefits of digital biomarkers and artificially powered IOT devices. In Part II, we discuss consumer protections under current healthcare laws, including HIPAA. In Part III, we briefly summarize the extraordinary value presented to cybercriminals by healthcare data and look to the current state of the healthcare industry. In Part IV, we look to the false sense of trust consumers have in the privacy and security of their healthcare information. In our conclusion, we look to the future of wearable devices and how the data they generate and retain should be stored and protected in light of its sensitive nature.

---

[3] Justin D. Evans, *Improving the Transparency of the Pharmaceutical Supply Chain through the Adoption of Quick Response (QR) Code, Internet of Things (IoT), and Blockchain Technology: One Result: Ending the Opioid Crisis*, 19 PITT. J. TECH. L. & POL'Y 35 (2019).

[4] Sohini Mitter, *31 Billion 'Connected' Devices Expected in 2018, Will this be the Year of IoT?*, YOURSTORY (Feb. 9, 2018), https://yourstory.com/2018/02/will-31-billion-connected-devices-expected-2018-will-year-iot.

[5] Johanna Mischke, *The State of Wearable Technology in Healthcare: Current and Future*, WEARABLE TECHNOLOGIES (Oct. 4, 2018), https://www.wearable-technologies.com/2018/10/the-state-of-wearable-technology-in-healthcare-current-and-future.

[6] Robert Sanders et al., *Data Storage and Retrieval by Implantable Pacemakers for Diagnostic Purposes*, *7* PACING AND CLINICAL ELECTROPHYSIOLOGY 1228, 1228–33 (1984).

[7] *Id.*; *see also* Stephen Armstrong, *What Happens to Data Gathered by Health and Wellness Apps?*, 353 BMJ 3406 (2016).

## PART I: BENEFITS OF IOT DEVICES

Personalized medicine has changed the way healthcare professionals and patients approach health.[8] Personalized medicine is a coordinated and user-centric approach to an individual patient's health.[9] Aggregating patient data in a centralized fashion allows patients to exercise greater autonomy when it comes to their healthcare.[10] IoT incorporation will likely result in economic and social benefits for all sectors of the healthcare industry, by facilitating the interaction between citizens, end users, governments, and corporations; thereby enhancing the goals of personalized medicine.[11] IoT devices employ algorithms which measure physiological, biological, and cognitive information and can provide physicians with real-time data on which to base a diagnosis. As the use of wearable and implants increases, physicians will gain a more complete picture of a patient's health.

The use of IoT devices can also allow patients to return home quicker after medical treatments; generally, telepath can reduce the overall cost of the hospital visit and increase the number of patients that can be seen by a single physician.[12] IoT devices allow for continuous virtual monitoring and require little intervention on the part of the physician, caregiver, or patient. Remote patient monitoring employs the use of smartphones and smart body sensors, which allow real-time data collected from the patient to be shared with their physician.[13] These devices will allow patients from all regions, rural and urban, to receive a more personalized solution to their medical needs, and this could help bridge medical disparities that arise due to location.[14] A prime example of such a device is the Dexcom Continuous Glucose Monitor, which is an integrated system for glucose measurement and automated insulin delivery.[15] Another example is the cardiac pacemaker, which is implanted in a patient's chest, allowing physicians and device manufacturers to interact with the pacemaker, including controlling, programming, and saving its data.

---

[8] Nicholas J. Schork, *Personalized Medicine: Time for One-Person Trials*, 520 NATURE 609, 609–11 (2015).

[9] *Id*.

[10] *Id*.

[11] *How IoT Is Changing the Science of Medicine*, FORBES (Sep. 14, 2018), https://www.forbes.com/sites/insights-inteliot/2018/09/14/how-iot-is-changing-the-science-of-medicine/#18526aef33e5.

[12] *Id*.

[13] Margaret Rouse, *Remote Patient Monitoring (RPM)*, SEARCHHEALTH IT, https://searchhealthit.techtarget.com/definition/remote-patient-monitoring-RPM (last updated April 2019).

[14] *Id*.

[15] Press Release, FDA, FDA Authorizes First Fully Interoperable Continuous Glucose Monitoring System, Streamlines Review Pathway for Similar Devices (Mar. 27, 2018), available at https://www.fda.gov/newsevents/newsroom/pressannouncements/ucm602870.htm.

*Digital Biomarkers*

Few patients survive pancreatic cancer because it is rarely detected early. With early detection, such a disease could be cured with immediate surgery.[16] The physical indications often associated with a person that has cancer do not arise until the cancer has progressed.[17] Unfortunately, the survival rate for pancreatic cancer after one year is only 20%, whereas only 7% of individuals are still alive five years after diagnosis.[18]

But imagine if a marker or indicator, already within the body, could detect cancer. How many lives could be saved by enabling patients to seek treatment earlier?[19] A biomarker does just that; it is a molecule that is secreted by the tumor or is secreted by the body itself in response to the presence of a tumor.[20] Biomarkers are released during certain points in time during a tumor's progression.[21] They are quantifiable characteristics of biological processes and have a direct relationship to medical signs, symptoms or clinical endpoints.[22] The current methods of diagnosing and following up with these patients are timely and costly. However, IoT devices allow physicians monitoring both patients suffering from chronic diseases and those who are susceptible to diseases like pancreatic cancer, to monitor their patients' biomarkers and act early.[23]

Increased data points and greater access to information have the potential to optimize and personalize treatment or therapy concepts by identifying critical points for intervention. IoT devices, many of which are already in the testing stage, are being used to monitor patients' nasal fluids, saliva, and blood for protein levels, glucose or other tumor markers like GPC1.[24] Glypican-1 (GPC1) is a cell surface protein of the heparan sulfate proteoglycan family that is overexpressed in the tissues for pancreatic cancer cells.[25] Detection of the overexpression of GPC1 at various critical points in

---

[16] *Prognosis,* HIRSHBERG FOUNDATION FOR PANCREATIC CANCER RESEARCH, http://pancreatic.org/pancreatic-cancer/about-the-pancreas/prognosis (last visited June 8, 2019).

[17] *Id*.

[18] *Id*.

[19] *Can Pancreatic Cancer Be Found Early*?, AMERICAN CANCER SOCIETY, https://www.cancer.org/cancer/pancreatic-cancer/detection-diagnosis-staging/detection.html (last updated Feb. 11, 2019).

[20] Christopher Kovalchick et al., *Can Composite Digital Monitoring Biomarkers Come of Age? A Framework for Utilization*, 1 J. CLINICAL & TRANSL. SCI. 373, 373–80 (2017).

[21] *Id*.

[22] Kyle Strimbu & Jorge A. Tavel, *What are Biomarkers*?, 5 CURR. OPIN. HIV AIDS 463, 463–66 (2010).

[23] *Id*.

[24] *Id.*; *see also* Jian Li et al., *The Clinical Significance of Circulating GPC1 Positive Exosomes and its Regulative MiRNAs in Colon Cancer Patients,* 8 ONCOTARGET 101189, 101189_202 (2017).

[25] Haizhen Lu et al., *Elevated glypican-1 expression is associated with an unfavorable prognosis in pancreatic ductal adenocarcinoma,* 6(6) CANCER MEDICINE 1181, 1181 (2017).

early stages can result in an easier and more effective treatment.[26] Studies have shown that the inhibition of the GPC1 protein in pancreatic tumors decreases the overall growth of the tumor.[27] If IoT devices can monitor individuals and catch subtle signs of illness early, there is a very real possibility that many life-threatening illnesses and even deaths can be prevented.

*Artificially Powered IoT Devices*

With the evolution of artificial intelligence (AI), personalized medicine is on the rise. AI can store, integrate, and analyze the incredible amounts of data accrued by such devices.[28] AI will be used to identify patterns within the high volume of genetic data sets, allowing for the prediction of a patient's probability of developing certain diseases, and to assist physicians with designing potential therapies.[29]

Studies done on the error rates of cancer diagnoses have found that as many as one in four individuals suffer from inadequate physical examinations and incomplete diagnostic tests.[30] AI-powered IoT devices have the capability to help in this arena. For example, AI will soon be capable of linking to tools that are able to analyze compounds in human breath, detecting illnesses like cancer early on.[31] AI tools have been, and will continue to be, trained with data from patients with various types of cancers.[32] Cancers often produce a distinctive smell of volatile organic compounds.[33] AI will one day be able to decipher chemical compounds in breath samples to identify those being emitted by the tumor.[34] AI detection tools will not be used to replace physicians, but rather will function as supportive tools.[35] Such AI tools can also be

---

[26] *Id.*

[27] *Id.* at 1183.

[28] Travis B. Murdoch & Allan S. Detsky, *The Inevitable Application of Big Data to Health Care*, 309 JAMA 1351, 1351–52 (2013).

[29] Jennifer Bresnick, *Top 12 Ways Artificial Intelligence Will Impact Healthcare*, HEALTH IT ANALYTICS (Apr. 30, 2018), https://healthitanalytics.com/news/top-12-ways-artificial-intelligence-will-impact-healthcare.

[30] Joe Cantlupe, *Cancer Misdiagnosis Surprisingly Common*, HEALTHLEADERS (Feb. 7, 2013), https://www.healthleadersmedia.com/strategy/cancer-misdiagnoses-surprisingly-common.

[31] Andrea Soltoggio, *Artificial Intelligence May Be Able to Smell Illnesses in Human Breath*, SMITHSONIAN.COM (Jun. 11, 2018), https://www.smithsonianmag.com/innovation/-artificial-intelligence-may-be-able-to-smell-illnesses-in-human-breath-180969286/#skzVl7m1ABdIe2XL.99.

[32] *Id*.

[33] *Id*.

[34] *Id.*

[35] Charles Taylor, *How Artificial Intelligence Will Shape the Physician Toolkit in 2019*, MEDCITY NEWS (Jan. 6, 2019), https://medcitynews.com/2019/01/how-artificial-intelligence-will-shape-the-physician-toolkit-in-2019.

used to autonomously analyze MRI scans that traditionally take physicians hours to evaluate.[36]

With many diseases like cancer, there is a very narrow window in which a therapeutic agent will prove effective.[37] Insufficient dosing or targeting is often associated with higher rates of toxicities or metastasis.[38] Therefore, there is an increasing need to develop strategies for determining appropriate doses and dosing windows.[39] There are many factors that affect the pharmacokinetics of detecting an appropriate dose or dosing window including ethnicity, age, gender, concomitant medication, and weight.[40] AI could investigate the clinical and genetic factors associated with appropriate dosing and timing.[41]

AI, in combination with the Internet of Things, will help patients play a more active role in their own health.[42] Patients will soon have their records stored on a single platform for all of their doctors to access when diagnosing or prescribing medication.[43] Patients will also soon be able to leverage IoT tools to help monitor their glucose levels and heart rates, allowing them to respond to potential issues earlier.[44] By having more autonomy over their own health, patients can obtain reliable second and third opinions by granting access to all of their medical records in real-time.[45]

## PART II: HIPAA AND OTHER PRIVACY AND SECURITY SAFEGUARDS

Personal medical information is not necessarily private. In 2018, there were approximately 221 data breaches of more than 500 records reported to the Department of Health and Human Services' Office for Civil Rights.[46] As a result, more than six million patients had their personal data stolen.[47] Interestingly, many of the devices

---

[36] *Id*.

[37] Sharon Rosen, *Pharmacogenomics: Finding the Right Drug, Dose for Cancer Therapy*, INDIVIDUALIZED MED. BLOG (Nov. 2018), https://individualizedmedicineblog.mayoclinic.org-/2018/11/05/pharmacogenomics-finding-the-right-drug-dose-for-cancer-therapy/.

[38] *Id*

[39] *Id*.

[40] *Id*.

[41] *Id*.

[42] Jo Best, *AI and the NHS: How Artificial Intelligence Will Change Everything for Patients and Doctors*, ZDNET (Nov. 15, 2018), https://www.zdnet.com/article/ai-in-the-nhs-how-artificial-intelligence-will-change-everything-for-patients-and-doctors.

[43] *Id*.

[44] *Id*.

[45] *Id*.

[46] *July 2018 Healthcare Data Breach Report,* HIPAA JOURNAL (Aug. 24, 2018), https://www.hipaajournal.com/july-2018-healthcare-data-breach-report/.

[47] Best, *supra* note 42. Interestingly, the healthcare industry is well known to have the highest number of breaches initiated by insiders. It is reported that around 58% of healthcare system breaches are initiated by corporate insiders.

discussed in this note are not covered by HIPAA, which means the data they accrue is not subject to its stricter security and privacy parameters.

In order to fall under Health Insurance Portability and Accountability Act of 1996 (HIPAA) safeguards, healthcare data must fulfill two general requirements. First, the data must be personally identifiable, and second, it must be maintained by a HIPAA covered healthcare provider, health plan, or healthcare clearinghouse.[48] While a great deal of healthcare data does fall into the personally identifiable information realm, the second requirement largely disallows HIPAA from protecting information accrued by healthcare wearables. The devices and companies that manufacture wearables and implants generally do not fall under the respective umbrellas of a healthcare provider, health plan, or healthcare clearinghouse.

While it is possible to expand HIPAA to cover commercial healthcare data, that arena may need to be addressed through separate legislation. At the moment, the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) have largely taken on the task of regulating the healthcare wearable space.[49] While the FTC prohibits companies from engaging in "unfair or deceptive practices" and has also issued guidance related to biometric information retention, so far, much of their work has focused on the consumer facial recognition technology space.[50]

The FCC has created the Connect2HealthFCC senior task force.[51] However, the task force is largely preoccupied with growing the healthtech space, and less focused on the safety and security of the devices themselves.[52] FCC's Chairman Pai, in a public statement regarding the promotion of Connect2HealthFCC's telehealth project, noted that, "patients can use remote monitoring and mobile health applications through connected devices to track their health and receive care wherever they are."[53] While the FCC's role is to regulate interstate communications, and to promote public safety, the potential dangers associated with heathtech devices have escaped Pai's attention. In a statement about the task force, he mentioned wanting to help benefit "low-income consumers, especially those in rural areas," who "lack access to affordable

---

[48] Daniel J. Gilman & James C. Cooper, *There is a Time to Keep Silent and a Time to Speak, the Hard Part is Knowing Which is Which: Striking the Balance Between Privacy Protection and the Flow of Health Care Information*, 16 MICH. TELECOMM. & TECH. L. REV. 279, 302 (2010).

[49] FTC, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD: STAFF REPORT TO FEDERAL TRADE COMMISSION 3 (2015), available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[50] Press Release, FTC, FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies (Oct. 22, 2012), available at https://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition.

[51] *Connect2HealthFCC,* FCC, https://www.fcc.gov/about-fcc/fcc-initiatives/connect2-healthfcc (last visited May 27, 2019).

[52] Fed. Commc'n Comm'n, National Broadband Plan: Connecting America (2010), available at https://www.fcc.gov/general/national-broadband-plan.

[53] *Id.*

broadband."[54] Because the task force is driven by a desire for a national broadband plan, it engages in little discussion concerning the regulation of IoT wearables and implants.[55]

Given the holes in the current regulatory scheme, it is of little surprise that multiple federal agencies have had to pick up slack in the healthtech space. The Government Accountability Office (GAO), prodded by Congress, asked the Food and Drug Administration (FDA) to investigate the potential risk of hacking of pacemakers.[56] According to the GAO, the FDA's responsibilities "include premarket and postmarket oversight spanning, for example, both premarket review of devices and postmarket surveillance (the collection and analysis of data on marketed devices)... In 2009, GAO added FDA's oversight of medical products, including devices, to its list of high-risk areas warranting attention by Congress and the executive branch."[57] That investigation resulted in the FDA recalling more than half a million pacemakers.[58] The recall was limited to devices on hand, as the FDA found that the recall would require an invasive and dangerous medical procedure for more than half a million people.[59] Instead of issuing a recall for the already-implanted devices, the FDA required manufacturers to issue updates to patch the potential security holes.[60] With current safety measures largely inadequate, including the largely inapplicable safety measures granted under HIPAA and the unwatchful eye of the FCC and FDA, there needs to be a regulatory scheme in place to protect heathtech consumers.

## PART III: CYBERCRIME & THE CURRENT STATE OF THE HEALTH INDUSTRY

Hospitals and other healthcare providers are under constant attack by cybercriminals, who are looking to extract patient data. Healthcare professionals are sitting on a treasure trove of data and do not always practice the best security protocols. Interestingly, patient data is worth more to cybercriminals than credit card numbers.[61]

---

[54] Press Release, FCC, Statement of FCC Chairman Ajit Pai, (Aug. 2, 2018), available at https://www.fcc.gov/document/fcc-seeks-comments-launching-telehealth-pilot-program/pai-statement.

[55] *Id*.

[56] FCC, PROMOTING TELEHEALTH FOR LOW-INCOME CONSUMERS, FCC 18–213 (2018), available at https://docs.fcc.gov/public/attachments/DOC-352540A1.pdf.

[57] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-09-370T, MEDICAL DEVICES: SHORTCOMINGS IN FDA'S PREMARKET REVIEW, POSTMARKET SURVEILLANCE, AND INSPECTIONS OF DEVICE MANUFACTURING ESTABLISHMENTS (2009); *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12- 816, MEDICAL DEVICES: FDA SHOULD EXPAND ITS CONSIDERATION OF INFORMATION SECURITY FOR CERTAIN TYPES OF DEVICES (2012).

[58] Alex Hern, *Hacking Risk Leads to Recall of 500,000 Pacemakers Due to Patient Death Fears*, THE GUARDIAN (Aug. 31, 2017), https://www.theguardian.com/technology/2017-/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update.

[59] *Id.*

[60] *Id.*

[61] Caroline Humer & Jim Finkle, *Your Medical Record is Worth More to Hackers Than Your Credit Card*, REUTERS (Sept. 24, 2014), https://www.reuters.com/article/us-cybersecurity-

Cybercriminals can sell credit information for 10 to 15 cents each, whereas medical records can be sold for as much as $30 to $1000 dollars a person.[62] Access to patient files gives cybercriminals access to prescriptions and to medical equipment that can be re-sold.[63] Cybercriminals use tools like ransomware to exploit vulnerabilities in a hospital's network by employing efforts to target hospital staff.[64]

For example, two employees of Morehead Memorial Hospital in Eden, North Carolina fell victim to such an attack, which resulted in cybercriminals gaining unauthorized access to their work email accounts.[65] These work accounts had access to protected health information of patients and sensitive information regarding other employees of the hospital.[66] The patient protected information included patient names, health insurance payment summaries, health insurance information, treatment plans, and some social security information.[67] The overwhelming amount of PII available to cybercriminals is astounding, and without protection this information is highly vulnerable to exploitation.

## PART IV: A FALSE SENSE OF TRUST

The world is currently experiencing a digital revolution, as access to the internet and technology has increased significantly across age groups. As a result of technological advancement, users have developed a false sense of trust in the various tools that we use on a daily basis. Our increased reliance on technology has created more and more endpoints, whereby information can be accessed. This creates a vulnerability that is threatening to disrupt the trust that people have in this ever-connected world.

Corporations have become alluring repositories for hackers, who employ various tools to gain access to their clients' information. One of the most utilized techniques by hackers to gain access to corporations' information is malware.[68] Ransomware is a type of malware that hackers employ to gain access to a corporation's clients'

---

hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924.

[62] Mariya Yao, *Your Electronic Medical Records Could Be Worth $1000 to Hackers*, FORBES (Apr. 14, 2017), https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#45cb380950cf.

[63] *Id*.

[64] *Id.*

[65] Taft Wireback, *Morehead Hospital Adds Data Breach Issues to Bankruptcy Process*, WINSTON-SALEM JOURNAL (Nov. 29, 2017), https://www.journalnow.com/news/local-/morehead-hospital-adds-data-breach-issues-to-bankruptcy-process/article_dcbfd48d-9143-50b0-b49c-b35e2efdc580.html

[66] *Id*.

[67] *Id.*

[68] Amy M. Gordon et al., *Ransomware Attacks under HIPAA and State Data Breach Notification Laws*, LEXIS PRAC. ADVISOR J. 7540 (2017).

information.[69] Other attacks have used massive botnet-powered malware to conduct denial-of-service (DDoS) attacks using thousands of IoT devices to exploit vulnerabilities of various systems to cripple websites.[70] There are over one-hundred million healthcare IoT devices that are installed daily around the world; of the projected twenty billion IoT devices that will be in use by 2020, 161 million of them will be used for healthcare-related purposes.[71] All healthcare IoT devices, from pacemakers to remote patient monitoring devices, are vulnerable to potential attacks from cybercriminals or cyber terrorists, as they have created a virtual portal into that user's physical and mental healthspace.

Attacks using IoT devices will continue to evolve and can be used to target patient data or patient devices. In fact, during a DefCon and Blackhat event, researchers were able to show how they could hack pacemakers, insulin pumps, and alter patients' vital signs in real time.[72] Blackhat conference lecturers discussed how hackers can hack and take control of pacemakers, ultimately causing them to over-deliver or deny delivery of life-saving shocks that patients rely on for survival.[73] Interestingly, former Vice President Dick Cheney had his own pacemaker's wireless capability disabled to prevent potential cyber attacks.[74]

With the rapid development of IoT technologies, hospitals are no longer only collecting data from physicians but also receiving data self-accrued by patients.[75] Organizations are often unaware that there are a large number of IoT devices connected to their system. In fact, each hospital bed has, on average 10 to 15 connected

---

[69] *Id.*

[70] Russ Banham, *DDoS Attacks Evolve to Conscript Devices onto the IoT,* FORBES (Feb. 4, 2018), https://www.forbes.com/sites/centurylink/2018/02/04/ddos-attacks-evolve-to-conscript-devices-onto-the-iot/#674514616aaa.

[71] *Estimated Healthcare IoT Device Installations Worldwide from 2015 to 2020*, STATISTA, https://www.statista.com/statistics/735810/healthcare-iot-installations-global-estimate/ (last visited June 8, 2019).

[72] Ms. Smith, *Hacking Pacemakers, Insulin Pumps and Patients' Vital Signs in Real Time,* CSO (Aug. 12, 2018), https://www.csoonline.com/article/3296633/hacking-pacemakers-insulin-pumps-and-patients-vital-signs-in-real-time.html.

[73] *Id.*

[74] Lisa Vaas, *Doctors Disabled Wireless in Dick Cheney's Pacemaker to Thwart Hacking*, SOPHOS (Oct. 22, 2013), https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/. Cheney became aware of the potential after being informed about a pacemaker assassination attempt depicted on the show *Homeland*. *See also How Medical Devices like Pacemakers and Insulin Pumps Can Be Hacked*, CBS NEWS (Nov. 8, 2018), https://www.cbsnews.com/news/cybersecurity-researchers-show-medical-devices-hacking-vulnerabilities/. Hackers showed CBS "how they can send a wireless signal, telling the pump to deliver the wrong amount of insulin to a patient nearby who might be wearing it. They also found vulnerabilities in a Medtronic pacemaker that could allow a hacker to reprogram the device from anywhere – disrupting a patient's heart rhythms in a way that could hurt or kill them."

[75] Bob Brown, *How to Keep Terrifying Medical Device Hacks from Becoming Reality*, NETWORK WORLD (Sept. 25, 2016), https://www.networkworld.com/article/3123761/how-to-keep-terrifying-medical-device-hacks-from-becoming-reality.html.

devices.[76] One of the hurdles for properly protecting a hospital is understanding that securing medical devices is different than managing a hospital's traditional IT system.

## PART V: IMPROVING IOT DEVICES

The global IoT device market is projected to grow from 249 billion dollars in 2018 to 457 billion dollars in 2020, causing many healthcare and medical device manufacturers to race to develop smarter and more connected devices.[77] When developing these devices, manufacturers and healthcare corporations will have to continually update their devices' firmware and security protocols to prevent them from being used to conduct attacks, including DDoS attacks against organizations, eavesdropping on network traffic, or compromising other devices on the same network segment.[78]

To best protect patient data, manufacturers and healthcare corporations will need to secure the confidentiality, integrity, and availability of the data collected by, stored on, processed by, or transmitted to or from IoT devices. Strengthening cybersecurity measures should be of utmost importance to healthtech companies, as well as regulatory agencies like the FCC and FDA. The creation of a taskforce that does more than just promote the adoption of wearable healthtech devices will allow for more targeted regulation of the data-driven space. Allowing researchers to more freely access the information they need, while disallowing cybercriminal access to PII, should be the goal of those acting in the interests of the consumer. Whether a new regulatory scheme needs to be created, or whether current statutes and agencies can begin to effectively address consumer concerns, there needs to be a better solution to the massive amount of personal data that heathtech companies hold so precariously. A safety and consumer-first approach to IoT devices will allow for products that not only save lives, but will also ensure security and privacy.

### *Identifying Potential Discrimination and Ethics Violations*

We are generating, collecting and sharing more information than ever before, and this includes information that may be tied to improving patient health. Although AI has the potential to transform the way patients approach health, it also raises important issues regarding discrimination and ethics violations, in addition to privacy and security issues.

For AI systems to be properly educated, they need to access vast amounts of patient data from a central repository. Storing such sensitive data in a single location creates an attractive target for hackers. While, machine learning requires such data sets for

---

[76] Julian Alvarado, *The IoT Within Us: Network-Connected Medical Devices,* SYNOPSYS (Sept. 14, 2018), https://www.synopsys.com/blogs/software-security/network-connected-medical-devices/.

[77] George Grachis, *The IoT Tsunami is Coming,* CSO (Oct. 17, 2018), https://www.csoonline.com/article/3314558/the-iot-tsunami-is-coming.html.

[78] Elizabeth O'Dowd, *Protecting Health IT Infrastructure from DDoS Attacks*, HIT INFRASTRUCTURE (Jan. 3, 2017), https://hitinfrastructure.com/news/protecting-health-it-infrastructure-from-ddos-attacks.

training and validation, more secure application programming interfaces ("API's") would allow researchers to access the data without as many drawbridges down for potential hackers. Another possible technological solution could rest in the use of cryptography, whereby information is shared across a peer to peer ledger, rather in a centralized location.[79] Blockchain allows for different subsets of data to be better anonymized.[80] Because all data tied to a single individual is not kept in one location, it is harder to piece together one individual's identity. The concept of utilizing blockchain for healthcare data is new and warrants further exploration.

Medical ethics, and concerns regarding big data, is not a new area of contention in the medical community. Henrietta Lacks, during the course of her cancer treatment at Johns Hopkins University, had her cancerous cervical cells scraped.[81] Mrs. Lack's cancer cells, called HeLa cells, were generated into a cell line and studied indefinitely without proper permission or compensation.[82] While her cells yielded incredible returns for medical innovation, Henrietta's contribution, or lack thereof since her cells were taken without her knowledge, did little to change her life as an impoverished African American tobacco farmer. The story of Henrietta's cells raises questions concerning ethical experimentation. Data, like Henrietta's cells, is a valuable commodity, and is often taken from individuals who are both uncompensated and unaware. There is fear that patient data will take a similar journey as Henrietta's cells, allowing data to be used by researchers without the consent of the patient.[83] In fact, in a poll done by Revolution Analytics, which surveyed data scientists, researchers determined that nine out of ten scientists felt that patients should worry about organizations collecting their data.[84] These scientists felt that there should be ethical considerations implemented to help data scientists and organizations know the proper way to navigate patient data.[85]

First, to fix the bias that is associated with the implementation of AI, we must admit that there is a problem associated with chosen data sets. Second, for AI to live up to its true potential, developers must be transparent about the inner workings of their programs. It is important that the members of the AI community recognize and emphasize the use of ethical design to prevent and correct for bias in machine learning algorithms. Users of AI tools need to hold developers accountable. Developers also

---

[79] Ashutosh D. Dwivedi et al., *A Decentralized Privacy-Preserving Healthcare Blockchain for IoT,* 19 SENSORS 2 (2019), available at https://www.ncbi.nlm.nih.gov/pmc/articles-/PMC6359727/pdf/sensors-19-00326.pdf.

[80] *Id.* at 5.

[81] DeNeen L. Brown, *Can the 'Immortal Cells' of Henrietta Lacks Sue for Their Own Rights?*, WASH. POST (June 25, 2018), https://www.washingtonpost.com/news/retropolis-/wp/2018/06/25/can-the-immortal-cells-of-henrietta-lacks-sue-for-their-own-rights/?utm_term=.34e8ca9f3e87.

[82] *Id.*

[83] *Id.*

[84] *Results of Survey of Statisticians at JSM 2013 Conference*, REVOLUTIONS (Sept. 12, 2013), https://blog.revolutionanalytics.com/2013/09/statistician-survey-results.html. Patients need to know who has the ability to use their data down the line because ultimately the data is owned by the patient. Patients pay the hospital to treat them, so they should be brought into all conversations surrounding their data.

[85] *Id.*

need allies in the field to help them determine which data should be included in the teaching set for the AI tool, and which data should be used for validation. It is also important to provide tutorials and tools to help less experienced data scientists and engineers identify and remove bias from their training data.

## CONCLUSION

While HIPAA protects the contents of hospital records, there is no such legislation protecting data accrued by healthtech wearables and implants. While the FDA, FCC, and FTC have all had a hand in regulating healthtech devices, there is no overarching federal legislation that protects the privacy and security of devices that are accruing just as much, if not more, health data on patients than is traditionally collected and retained by hospitals. While HIPAA offers protections in the hospital and insurance arena, all other healthcare data is left vulnerable within a deregulated space.

Legislation drafted to regulate IoT security and privacy must acknowledge the ramifications of a data breach in the healthtech space, and manufacturers of healthcare products must be given a clear regulatory path to follow. When developing IoT products, manufacturers need to think security by design, allowing for swift update patches for any security holes discovered in their products' software. Manufacturers or a government agency should also implement a reporting system that allows consumers and other agencies to report flaws immediately.

The world is rapidly progressing into the digital age, but with such progress comes exploitable vulnerabilities. It is important that healthcare data is not compromised by the massive push towards innovation in the medical space. Current laws governing privacy and security of medical information do not apply to IoT healthcare devices. Increased legislation in this space, as well as recognition by companies that the data they are accruing is incredibly valuable, and therefore vulnerable, would go a long way in ensuring that IoT devices live up to their promise.