SMU Science and Technology Law Review

Volume 25 | Number 1 Article 3

2022

Oculogica: An Eye-Catching Innovation in Health Care and The Privacy Implications of Artificial Intelligence and Machine Learning in Diagnostics For The Human Brain

Samantha V. Ettari
Perkins Coie LLP

Elijah Roden
Perkins Coie LLP

Vishal Ahuja
Southern Methodist University

Uzma Samadani
University of Minnesota

Recommended Citation

Samantha V. Ettari et al., *Oculogica: An Eye-Catching Innovation in Health Care and The Privacy Implications of Artificial Intelligence and Machine Learning in Diagnostics For The Human Brain*, 25 SMU SCI. & TECH. L. REV. 23 (2022)
https://scholar.smu.edu/scitech/vol25/iss1/3

Oculogica: An Eye-Catching Innovation in Health Care and the Privacy Implications of Artificial Intelligence and Machine Learning in Diagnostics for the Human Brain

Samantha V. Ettari, Elijah Roden,** Vishal Ahuja,*** Uzma Samadani*****

ABSTRACT

This article explores the use of Artificial Intelligence (AI) in emerging eye-tracking diagnostic technology, with a focus on both the patient data privacy and security regulations that firms, specifically device inventors and manufacturers, may face and how such firms can address the developing privacy and regulatory legal challenges. In addition, we discuss the ethical considerations of algorithmic bias, the impact such biases have on society and

DOI: https://doi.org/10.25172/smustlr.25.1.3

* Senior Counsel in the Privacy and Data Security Group at Perkins Coie LLP. Samantha counsels clients on privacy, data security, and data management and has significant experience with legal and practical risk counseling, often in the context of mergers, acquisitions, and technology-driven strategic and investment transactions. She advises clients on domestic and international privacy statutes and regulations, as well as cross-border transfers of data and the use of big data sets, including biometrics and other sensitive data.

** Attorney in the Technology Transactions & Privacy Group of Perkins Coie LLP. Elijah advises clients of various sizes on legal issues related to innovative solutions in technology and privacy, including technology-driven transactions, privacy, and security. He is a Certified Information Privacy Professional for the European Union (CIPP/E) and for the United States (CIPP/US).

*** Associate Professor of Information Technology and Operations Management at Southern Methodist University's Cox School of Business and an Adjunct Faculty of Clinical Sciences at University of Texas Southwestern Medical Center. Vishal's research focuses on developing decision analytic tools that can be easily implemented by healthcare professionals and policymakers to improve patient outcomes, advance the quality of care, and enhance the efficiency of care delivery.

**** Associate Professor at the University of Minnesota, Department of Bioinformatics and Computational Biology, and Staff Neurosurgeon at Minneapolis VA HealthCare System. Her research focuses on brain and spinal cord injury.

The authors thank Dr. Rosina Samadani for contributing her extensive knowledge concerning the use of AI in medical diagnostics and the development of privacy compliance and ethical AI programs at medical device startups. This article was drafted with the significant assistance of Cayro Bustos (JD Candidate at SMU Dedman School of Law), Danielle Harlan (JD Candidate at SMU Dedman School of Law, and Moses Washington (JD Candidate at North Carolina Central University School of Law), 2022 Summer Associates in the Perkins Coie LLP Dallas Office. Their assistance was invaluable to the preparation of this article.

emerging technology, along with specific actions companies should take to maximize patient outcomes. Lastly, we offer a case study of Oculogica, an emerging digital health technology company—and its medical device (EyeBOX) – to illustrate how digital health firms can enhance patient outcomes, while ensuring data security and privacy, while simultaneously promoting responsible development of advanced algorithms for diagnostic AI.

INTRODUCTION

Each year in the United States, approximately 1.7 to 3.8 million people suffer concussions.[1] Approximately 75% to 90% of the 1.4 million people that die or are treated in hospitals for traumatic brain injuries (TBIs) suffer from concussions or mild TBIs (mTBIs).[2] However, many mTBIs are not treated due to challenges in diagnosis. "Conventional computed tomography (CT) and magnetic resonance imaging (MRI) scans almost always appear normal after concussions, even after repeated concussions."[3] Diagnosing a concussion is further complicated by patients obscuring symptoms from medical professionals, a lack of capacity to communicate effectively, or in-

[1] Nitin Agarwal et al., *Sports-related Head Injury*, Am. Ass'n of Neurological Surgeons, https://www.aans.org/Patients/Neurosurgical-Conditions-and-Treatments/Sports-related-Head-Injury [https://perma.cc/2EBW-DSFX]; *Concussions: Symptoms, Treatment and What You Need to Know*, UT Health San Antonio (Mar. 1, 2022), https://www.uthscsa.edu/patient-care/physicians/news-item/concussions-symptoms-treatment-and-what-you-need-know [https://perma.cc/Z3DV-DXEU].

[2] Press Release, CDC, CDC Announces Updated Information to Help Physicians Recognize and Manage Concussions Early (Jun. 7, 2007), https://www.cdc.gov/media/pressrel/2007/r070607.htm [https://perma.cc/Y9W5-UA7V].

[3] Charles H. Tator, *Concussions and Their Consequences: Current Diagnosis, Management and Prevention*, 185 CMAJ 975, 975–79 (2013).

herent bias in doctors or medical equipment.[4] Although mTBIs may resolve without treatment, "concussions may have substantial, long-term consequences at any age," and "young adults who sustain concussions are at relatively high risk for comorbid events."[5]

To illustrate, imagine the following scenario: a young woman of color with limited English proficiency is transported to a hospital's emergency room.[6] She was found unconscious outside at the bottom of a staircase, but paramedics are unaware of further details, such as whether she fell, was intoxicated, or suffered from mental illness. She arrives in the emergency room and appears confused and disoriented, pulling at a cervical collar provided by paramedics. While able to provide her name, she continues to attempt to remove the collar and is unable or unwilling to communicate when medical professionals seek additional information. Complicating her diagnosis and treatment, internal biases may lead medical professionals to assume characteristics about her, such as suspecting comorbid psychiatric diagnoses, intoxication or drug impairment, based on race, ethnicity, socioeconomic status, or other factors,[7] when, in fact, the woman was suffering from an mTBI.

Oculogica aims to address misdiagnosis of mTBI through its non-invasive EyeBOX device, which uses eye-tracking to detect abnormal eye movement and infer characteristics of brain function.[8] Cleared by the Food and

[4] *Id.*; *see also* William J. Hall, et al., *Implicit Racial/Ethnic Bias Among Health Professionals and Its Influence on Health Care Outcomes: A Systematic Review*, 105 AJPH e60, e61 (2015).

[5] Tim Sullivan, *Concussion Consequences*, HARV. MED. SCH. (Mar. 4, 2021), https://hms.harvard.edu/news/concussion-consequences [https://perma.cc/CKE2-BLQK].

[6] *See* Jeffrey Bazarian, et al., *Ethnic and Racial Disparities in Emergency Department Care for Mild Traumatic Brain Injury*, 10 ACAD. EMERG. MED. 1209, 1210–11 (2003) https://www.frontiersin.org/articles/10.3389/fmed.2020.00300/full#B15. African Americans are less likely to receive care from a staff physician than white individuals. Racial profiling exacerbates misdiagnoses, especially when an emergency room is particularly busy or sees high number of intoxicated individuals.

[7] *See* Bazarian, *supra* note 6; *see also* Xingyu Zhang, et al., *Trends of Racial/Ethnic Differences in Emergency Department Care Outcomes Among Adults in the United States from 2005 to 2016*, FRONTIERS IN MED. (2020), https://www.frontiersin.org/articles/10.3389/fmed.2020.00300/full (showing that Black patients were also 10% less likely than White patients to be admitted to the hospital and were 1.26 times more likely than White patients to die in the ED or hospital. Additionally, non-White patients are more likely to receive disparate treatment for many common symptoms, including brain injuries).

[8] *Brain Health Magazine: Neurosurgeon Leads the Way in Eye Tracking Diagnosis for Concussion*, OCULOGICA (Dec. 9, 2019), https://oculogica.com/neurosurgeon-leads-the-way-in-eye-tracking-diagnosis-for-concussion/ [https://perma.cc/JGC6-Y463].

Drug Administration (FDA) in December 2018, EyeBOX can assist with diagnosing concussions through a four-minute eye-tracking test,[9] and is roughly the size of a desktop computer.[10] Though some medical insurance companies still consider eye-tracking experimental—despite its FDA clearance—additional insurance coverage can dramatically increase the EyeBOX's use in clinical settings, including emergency rooms and urgent care centers.[11]In field use is also theoretically possible. In 2017, "an estimated 2.5 million high school students reported having at least one concussion related to sports or physical activity during the year."[12] Eye-tracking technology has uses beyond acute brain injury, and Oculogica has obtained patents to use the technology to detect glaucoma and cannabis-related impairment.[13]

Using EyeBOX to track eye movements for diagnostic purposes could raise various legal and ethical issues. To train machine learning models, companies need large volumes of new and varied data, but companies must obtain that data ethically, in compliance with applicable law, and using secure systems that restrict personal data use to the purposes stated at collection. As regulators and legislators promulgate new laws, as different data elements become available, and as products become more sophisticated, privacy and data security compliance become increasingly more complex.

For start-ups, competition for resources can be fierce and securing leadership support for privacy and ethical initiatives can be challenging. In February 2022, Drs. Rosina Samadani and Uzma Samadani, of Oculogica, Professor Ahuja Vishal of SMU's Cox School of Business, and members of Perkins Coie, including co-author Samantha Ettari, as panel moderator, presented a panel at the SMU's 2022 Science & Technology Law Review Symposium, tackling these issues. The panelists discussed the interplay between artificial intelligence (AI), machine learning (ML), algorithmic fairness, privacy by design (PbD), and healthcare innovations, concluding that data privacy and stewardship are critical to growth and trust in the healthcare sector. Building on that panel conversation, this paper discusses (1) creation of Oculogica and the technology underpinning EyeBOX; (2) privacy and se-

[9] *See* Tom Kertscher, *Identifying Concussions,* Northwestern Magazine (Fall 2021), https://magazine.northwestern.edu/people/oculogica-eyebox-concussions-rosina-samadani/ [https://perma.cc/LXJ4-DZYF]; *see also De Novo Classification Request for EyeBOX*, FDA, https://www.accessdata.fda.gov/cdrh_docs/reviews/DEN170091.pdf [https://perma.cc/QSQ2-Y7ZQ].

[10] *See Brain Health Magazine*, *supra* note 8.

[11] *See* Kertscher, *supra* note 9.

[12] *See* Lara DePadilla, *Self-Reported Concussions from Playing a Sport or Being Physically Active Among High School Students — United States, 2017*, CDC (Jun. 22, 2018), https://www.cdc.gov/mmwr/volumes/67/wr/mm6724a3.htm [https://perma.cc/4UXQ-JUHL].

[13] US Patent Nos. 11,013,441, 10,201,274, and 10,863,902.

curity challenges, as well as how to ethically use AI to enhance medical devices faced by emerging healthcare and medical device companies; and (3) how Oculogica strives to meet these challenges.

1. OCULOGICA AND THE EYEBOX[14]

The research for the technology behind the EyeBOX began in 2011 when Dr. Uzma Samadani realized that eye-tracking could detect abnormal eye movements classically associated with brain injury.[15] This research eventually led Dr. Uzma Samadani to develop, publish, and patent algorithms that track the relationship between ocular dysmotility and mTBIs. Oculogica views this technology as a way to perform a digital neurologic examination and objectively diagnose concussions.[16] In fact, Dr. Rosina Samadani benefited from the technology when she was struck in the head by an umbrella on the beach,[17] and her sister confirmed her diagnosis of concussion using the EyeBOX.[18]

Where similar devices on the market require a baseline ("an initial measurement of a condition that is taken earlier and used for comparison over time to look for changes"[19]) and primarily assess a patient's attention, EyeBOX provides an objective assessment without needing baseline data for a specific patient. EyeBOX analyzes the "function of cranial nerves" and all of the pathways in the brain that feed into those nerves,[20] providing "a physiologic indicator of brain function"[21] by measuring pupil size and "position over time, comparing the position to each other and to a normative database."[22] EyeBOX separately collects approximately 100,000 data points

[14] Dr. Uzma Samadani, a full-time neurosurgeon, founded Oculogica, which describes itself as a company that develops "innova[tive] eye-tracking products for improved brain health," Oculogica, *About Us*, https://oculogica.com/about-oculogica/ [https://perma.cc/9U98-CK94], in 2013. Luna Abrams, *Rosina Samadani, CEO of Oculogica*, VIMEO, https://vimeo.com/560222554. She later recruited her sister, Dr. Rosina Samadani, to be Oculogica's CEO in 2015. Robin Kazmier, *Looking Concussion in the Eye*, MIT TECH. REV. (Apr. 25, 2018), https://www.technologyreview.com/2018/04/25/240754/looking-concussion-in-the-eye/ [https://perma.cc/RZ7P-5KZ5].

[15] *See id.*

[16] *See id.*

[17] *Id.*

[18] *See* Kertscher, *supra* note 9.

[19] *Baseline*, NAT'L CANCER INST., https://www.cancer.gov/publications/dictionaries/cancer-terms/def/baseline [https://perma.cc/7X9C-R9TH].

[20] *See* Kertscher, *supra* note 9.

[21] Kazmier, *supra* note 14.

[22] Amy Zellmer, *Neurosurgeon Leads the Way in Eye Tracking Diagnosis for Concussion*, THE BRAIN HEALTH MAG. (Oct. 22, 2019), https://

that it feeds into algorithms in order to calculate "nearly 100 different metrics quantifying such things as speed, coordination, and range of motion."[23] This provides the opportunity to gain insight into a number of different characteristics associated with abnormal brain function, including, for example, whether a person has elevated pressure inside the skull from brain swelling or inability to coordinate their eye movements as an object moves closer.[24] In the development of EyeBOX, Dr. Uzma Samadani and her research team identified the most important metrics associated with mTBIs, and used those metrics to develop algorithms capable of scoring the severity of brain injuries.[25] The company, Oculogica, then took those algorithms and developed the EyeBOX. EyeBOX has applications not only for diagnosis of concussion, which is its FDA-cleared indication, but also for triage and monitoring of any potential neurologic emergency.

Currently, healthcare providers assess mTBIs based on history, physical, and neuropsychological examination. Imaging in acute brain injury is generally utilized to rule out the need for surgery, and CT scanning is the preferred modality because it is relatively quick and inexpensive. MRI scanning is time-consuming and not generally performed acutely for brain injury but is sometimes obtained when an etiology for the patient's fall or syncopal event is not found. CT and MRI scans do not detect multiple subtypes of physiologic brain injury or concussion.[26]

Brain injury is often classified using the Glasgow Coma Scale (GCS) which summarizes components of the physical examination.[27] Subjective measurements such as the GCS may lead to certain inequities when medical professionals evaluate certain types of patients. For example, the Institute of Medicine, acknowledging that the differences in healthcare occur in the broader context of socioeconomic inequity, notes that "[b]ias, stereotyping, prejudice, and clinical uncertainty on the part of healthcare providers" are key factors in contributing to racial and ethnic disparities in healthcare.[28]

thebrainhealthmagazine.com/concussion/neurosurgeon-leads-the-way-in-eye-tracking-diagnosis-for-concussion/ [https://perma.cc/CF3A-A7B5].

[23] Kazmier, *supra* note 14.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *How Do Healthcare Providers Diagnose Traumatic Brain Injury (TBI)?*, NICHD – Eunice Kennedy Shriver Nat'l Inst. of Child Health and Hum. Dev., https://www.nichd.nih.gov/health/topics/tbi/conditioninfo/diagnose [https://perma.cc/K4F5-MYRF]. GCS involves testing a person's responses in these categories and calculating a person's total performance. A score of 13 or higher indicates an MTBI, and the lower the score goes, the more severe the brain injury is.

[28] Alan Nelson, *Unequal Treatment: Confronting Racial and Ethnic Disparities in Health Care*, 94 J. Nat'l Med. Ass'n 666, 667 (2002), https://

Objective measurement has the potential to help address these issues by providing concrete data removed from subjective measures that is less susceptible to bias than current methods; however, if not utilized at all, they cannot mitigate against misdiagnosis.[29] AI is one way to address inequities that may result from subjective measurements, but even AI is not a panacea if the underlying data is biased.[30]

2. PRIVACY, SECURITY, AND ARTIFICIAL INTELLIGENCE COMPLIANCE

The use of Oculogica's eye-tracking technology for concussion detection in the Emergency Room, as well as potentially assessing substance impairment in the workplace, brings privacy, security, and ethical obligations.[31] The United States' current sectoral and state-by-state approach to privacy and security means each additional use case and data collection may bring additional compliance obligations. Small start-up medical device companies, faced with scarce financial and personnel resources, still must address those compliance and ethical obligations.

A. Privacy Laws

The United States, at the federal level, utilizes a framework of sectoral privacy laws and regulations applicable to different industries, with varied protections.[32] Some states have passed consumer privacy legislation—both omnibus (for example, the California Consumer Privacy Act (CCPA)) and

www.ncbi.nlm.nih.gov/pmc/articles/PMC2594273/pdf/jnma00325-0024.pdf [https://perma.cc/CAB7-LB5G].

[29] *Id.*

[30] James Manyika, Jake Silberg, & Brittany Preseten, *What Do We Do About Biases in AI?*, HARV. BUS. REV. (Oct. 25, 2019), https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai [https://perma.cc/9B94-QW4N].

[31] Oculogica has obtained patents for "measuring elevated intracranial pressure, biometric identification of patients, and glaucoma detection," in addition to the CannaBOX. *Oculogica Adds to IP Portfolio with Patent for Assessment of Impairment Due to Cannabis*, GLOBE NEWSWIRE (May 25, 2021), https://www.globenewswire.com/news-release/2021/05/25/2235748/0/en/Oculogica-Adds-to-IP-Portfolio-with-Patent-for-Assessment-of-Impairment-Due-to-Cannabis.html [https://perma.cc/5638-DEP6].

[32] Shawn M. Boyne, *Data Protection in the United States*, 66 AM. J. C 299, 302-5, 308, https://academic.oup.com/ajcl/article/66/suppl_1/299/5048964 [https://perma.cc/FYG6-AVTP] (listing federal sectoral privacy laws like HIPAA, the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), and the Video Privacy Protection Act (VPPA)).

data-category specific (for example, Illinois's Biometric Information Privacy Act (BIPA)).[33]

Although device manufacturers are not necessarily implicated by the Health Information Portability and Accountability Act (HIPAA), manufacturers still need to ensure they are creating devices that help "covered entities" comply with HIPAA's Privacy and Security Rules.[34] These rules require that covered entities and business associates take care to ensure that patients' personal data, termed "protected health information" (PHI) and "electronic protected health information" (ePHI), are safeguarded and protected from anticipated threats and/or impermissible uses and/or disclosures.[35] In practice, this requires encrypting devices,[36] regular security risk assessments,[37] and restricting access to PHI and ePHI.[38]

Additionally, the FDA guidelines on electronic records and electronic signatures apply to all medical device manufacturers under 21 CFR Part 11. This rule requires that device manufacturers implement necessary controls including; audits, system validations, electronic signatures, and documentation for the software involved in processing electronic data.[39] Compliance with 21 CFR Part 11 generally requires companies to encrypt data, limit the ability of unauthorized individuals to access materials, prevent improper al-

[33] *See*, *e.g.*, Cal. Civ. Code §§ 1798.100–1798.199; 740 Ill. Comp. Stat. Ann. 14/15.

[34] Only certain entities are covered by HIPAA, including covered entities and business associates. Covered entities include health plans, most health care providers, and health care clearinghouses. *Your Rights Under HIPAA*, HHS, https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html [https://perma.cc/9V34-E5RA].

[35] *Id.*

[36] *Lifespan Pays $1,040,000 to OCR to Settle Unencrypted Stolen Laptop Breach*, HHS (Jul. 27, 2020), https://public3.pagefreezer.com/content/HHS.gov/31-12-2020T08:51/https://www.hhs.gov/about/news/2020/07/27/lifespan-pays-1040000-ocr-settle-unencrypted-stolen-laptop-breach.html [https://perma.cc/8FUZ-X68H].

[37] *Health Care Provider Pays $100,000 Settlement to OCR for Failing to Implement HIPAA Security Rule Requirements*, HHS (Mar. 3, 2020), https://public3.pagefreezer.com/content/HHS.gov/31-12-2020T08:51/https://www.hhs.gov/about/news/2020/03/03/health-care-provider-pays-100000-settlement-ocr-failing-implement-hipaa.html [https://perma.cc/9C9J-UMGT].

[38] *$5.5 Million HIPAA Settlement Shines Light on the Importance of Audit Controls*, HHS (Feb. 16, 2017), https://www.hhs.gov/guidance/document/55-million-hipaa-settlement-shines-light-importance-audit-controls-0 [https://perma.cc/6RB7-X96K].

[39] Part 11, Electronic Records; Electronic Signatures – Scope and Application, FDA, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application#iiic [https://perma.cc/6BSG-NJBN].

tering of data, and ensure proper record retention.[40] These are all bedrock principles of any medical device privacy program.

Training is critical for individuals handling PHI and ePHI. The Collaborative Institutional Training Initiative (CITI) Program is a leading research ethics, compliance, and professional development education provider.[41] In 2001, the National Institutes of Health (NIH) began requiring individuals working on human subject research to complete this training.[42] CITI-trained individuals are taught to ensure ethical, professional, regulatory, and security compliance in the research setting.[43]

While eye-tracking data may call to mind regulations around "biometric data," Oculogica's EyeBOX does not collect retinal scans from its subjects; only eye movements and images of the eye region of the face are collected. As a result, no biometric-specific data privacy laws are currently implicated through the use of the EyeBOX.[44]

While eye-tracking data collected by clinical partners and from use of the EyeBOX implicates privacy and data security (as noted above), it also requires transparent notice and consent to data subjects (including patients and clinical study volunteers). Notice and consent present a unique set of challenges in eye-tracking. Because eye-tracking can reveal so much about its subject,[45] providers using Oculogica's EyeBOX will need to provide de-

[40] *A [Printable] 21 CFR Part 11 Compliance Checklist to Follow Step-by-Step*, QUALIO, https://www.qualio.com/blog/printable-21-cfr-part-11-compliance-checklist [https://perma.cc/683U-HV8E].

[41] Duke Office of Clinical Research, *CITI Training*, DUKE UNIVERSITY SCHOOL OF MEDICINE, https://medschool.duke.edu/research/research-support-offices/duke-office-clinical-research-docr/get-docr-support-clinical-7 [https://perma.cc/W7P5-HTB8].

[42] *Our History*, CITI PROGRAM, https://about.citiprogram.org/get-to-know-citi-program/ [https://perma.cc/7XZ4-3SC8].

[43] *Biomedical (Biomed) Comprehensive Course*, CITI PROGRAM, https://about.citiprogram.org/course/biomedical-biomed-basic/ [https://perma.cc/6Z6P-MGLJ].

[44] Oculogica also collects recordings of a subset of the face around the eyes for non-patients. The video data from these individuals come from un-injured volunteers who are not concussed. This data is used only for control purposes when developing the product form-factor itself, and not for clinical studies, and is collected with Institutional Review Board (IRB) approval. These recordings are unlikely to trigger any biometric-specific privacy laws. Volunteers provide informed consent to provide their eye tracking data to Oculogica, and they may withdraw their consent at any time.

[45] Jacob Kröger, Otto Hans-Martin Lutz, & Florian Müller, *What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking, Privacy and Identity Management. Data for Better Living: AI and Privacy*, in 576 IFIP ADVANCES IN INFO. AND COMMC'N TECH. 226, 227 (2020) (discussing uses of eye tracking for the diagnoses of disease, mental health conditions, and substance

tailed information to patients to obtain informed consent. Apart from diagnosing head injury, data from eye-tracking can provide information about several other intimate details about a person, such as emotional state, intoxication from alcohol or other drugs, drug withdrawal, medical conditions like multiple sclerosis, Alzheimer's disease, and Parkinson's disease, or mental health conditions like schizophrenia and depression.[46] Therefore, notice and consent forms should address all potential uses of the eye-tracking data, including uses for other diagnoses or testing.

Organizations that employ or manufacture medical diagnostic technology should also consider the potential complexities involved in providing notice, obtaining consent for explicit uses, and securing data. These organizations are encouraged to take steps to keep up with privacy and security laws as they come into effect, such as (1) consulting experts in the field; (2) hiring a privacy officer; (3) preparing, updating, implementing privacy and data security policies; (4) tracking and enforcing those policies through publications and the use of automated systems; and (5) learning how to adapt to changes in the law and data sources as they occur.[47]

B. Security

Like many other types of data, PHI is uniquely sensitive and susceptible to cyberattack and unauthorized access.[48] Medical devices, including those connected to the internet or housing/transferring troves of PHI, are targets. Healthcare providers may be more susceptible to cyberattacks because they

use disorders; as well as identification of personality traits; age; cognitive processes; and cultural affiliation).

[46] *Id.* at 233.

[47] *16 Ways Tech Leaders Can Keep Up With Data Privacy Laws*, FORBES (Sep. 22, 2010), https://www.forbes.com/sites/forbestechcouncil/2020/09/22/16-ways-tech-leaders-can-keep-up-with-data-privacy-laws/?sh=1cb0b28c2463. Recently, in the California Attorney General's updated enforcement report, the AG highlighted an enforcement action against a medical device manufacturer that did not provide data subjects with a clear opt-out mechanism from the sale of their personal data and impermissibly restricted the exercise of data subject rights under the applicable privacy laws. CCPA Enforcement Case Examples, Office of the Attorney General (Aug. 24, 2022), https://www.oag.ca.gov/privacy/ccpa/enforcement.

[48] Just recently, researchers discovered a breach of a biometric database with approximately 27.8 million records, including fingerprint data of over one million people, facial recognition information, as well as usernames and passwords. Jon Porter, *Huge Security Flaw Exposes Biometric Data of More than a Million Users*, THE VERGE (Aug. 14, 2019), https://www.theverge.com/2019/8/14/20805194/suprema-biostar-2-security-system-hack-breach-biometric-info-personal-data.

often employ outdated security systems and have limited personnel and resources dedicated to cybersecurity.[49]

In 2018, the FDA provided draft cybersecurity guidance for medical devices in response to growing cybersecurity threats in the healthcare industry.[50] The guidance suggested the implementation of a risk-based categorization of devices into separate tiers, patch and software updates to devices, a framework for designating "trustworthy" devices, and security considerations early in the device design process.[51] On April 8, 2022, the FDA issued an updated version of its 2018 cybersecurity guidance[52] for medical devices in response to growing cybersecurity threats in the healthcare industry.[53] This guidance recommends privacy and data security considerations in the design phase, as well as labeling and documentation to help streamline the premarket review process and ensure that medical devices can withstand potential cybersecurity threats.[54]

As privacy laws continue to evolve, particularly in relation to medical devices and technology, one area that scholars and practitioners note remains vulnerable is securing big data sets utilized in AI and ML. The Cloud Security Alliance (CSA) stated that "privacy laws need to be consistent and flexible to account for innovations in AI and ML. Current regulations have not kept up with changes in technology."[55] For example, HIPAA calls for data

[49] Lucas Mearian, *Hackers are Coming for Your Healthcare Records – Here's Why*, CSO (Jul. 1, 2016), https://www.csoonline.com/article/3090553/hackers-are-coming-for-your-healthcare-records-heres-why.html [https://perma.cc/28CN-E94G].

[50] Kristin Bryan, *FDA Publishes Draft Cybersecurity Guidance*, NAT'L L. REV. (Apr. 26, 2022), https://www.natlawreview.com/article/fda-publishes-draft-cybersecurity-guidance-medical-devices.

[51] *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, U.S. FOOD & DRUG ADMIN. (Oct. 2, 2014), https://www.fda.gov/media/86174/download [https://perma.cc/QM5M-NQ6Gf].

[52] This guidance replaces the prior guidance issued in 2018. The updated guidance implements prior comments and further emphasizes the importance in developing devices that are designed securely. Kristin Bryan, *FDA Publishes Draft Cybersecurity Guidance*, NAT'L L. REV. (Apr. 26, 2022), https://www.natlawreview.com/article/fda-publishes-draft-cybersecurity-guidance-medical-devices.

[53] U.S. Food & Drug Admin., Draft Guidance for Industry and Food and Drug Admin. Staff, *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions*, 87 FR 20873, 20873-20875 (proposed Apr. 8, 2022).

[54] *Id.*

[55] Jill McKeon, *AI in Healthcare Presents Need for Security, Privacy Standards*, HEALTH IT SEC. (Feb. 17, 2022), https://healthitsecurity.com/features/ai-in-healthcare-presents-need-for-security-privacy-standards [https://perma.cc/RHZ9-8DBT].

de-identification; however, it is possible that technology today (and certainly of the future) can link de-identified data resulting in identification if it is not anonymized correctly.[56] Thus, not only is it important for medical technology companies to keep up with their data privacy and security obligations, the increasing popularity of AI and big data sets support the need for industry standards.[57]

C. Compliance Programs

Guidance and legal frameworks for privacy and security impose obligations on companies to provide a floor for safeguarding sensitive data. Companies must find a way to implement those obligations into their day-to-day operations, but start-ups often lack the funding or personnel to prioritize developing a "privacy culture."[58] Privacy culture refers to "a common understanding across a company of privacy principles in general and their value to individuals."[59] A start-up may implement privacy training, but "training alone doesn't create culture."[60] Not recognizing the importance of privacy early on can prove costly later.[61] While not every start-up has the budget for a dedicated team of privacy professionals to address the constantly changing regulatory environment, building a privacy culture can help.[62]

A first step in creating a privacy culture at a start-up is clarifying how the company will integrate privacy into operations. One way that can be done is by developing, maintaining, and documenting privacy and information security policies, internal access and use guidelines, incident response plans, retention and systems backup policies, and other compliance efforts.[63]

A critical step in creating a privacy culture and program is for the start-up to adhere to the principle of "Privacy by Design" (PbD), which should

[56] Boris Lubarsky, *Re-Identification of "Anonymized" Data*, 1 Geo. L. Tech. Rev. 202, 206 (2017).

[57] McKeon, *supra* note 55.

[58] *See* Stephen Bolinger, *His Task? Start Up a Privacy Program at a Start-Up*, IAPP (Apr. 28, 2015), https://iapp.org/news/a/his-task-start-up-a-privacy-program-at-a-start-up-3/ [https://perma.cc/6HAF-T9C3].

[59] *Id.*

[60] *Id.*

[61] Stephanie Nguyen, *How Tiny Startup Teams Handle Big Privacy Issues*, Fast Co. (Jan. 24, 2020), https://www.fastcompany.com/90452270/how-tiny-startup-teams-handle-big-privacy-issues [https://perma.cc/E53T-44W7] (highlighting that the costs from these fines alone can surpass the cost of maintaining a privacy team).

[62] *See id.* (discussing how several start-ups have dealt with sensitive data and underscoring the importance of building privacy into the culture and implementing the concept of "Privacy by Design").

[63] *See* Bolinger, *supra* note 58.

embed principals of privacy, data minimization, transparency, and responsible retention and deletion, into the early stages of designing a product.[64] If an organization proactively thinks about privacy when designing technology, devices, procedures, or services, they are more likely to integrate privacy across the business and foster that culture successfully.[65]

A second step in creating a privacy culture is to give everyone baseline privacy training. This ensures that employees understand what privacy is, how it relates to their role, and why it matters.[66] This is especially important in companies where data is a major asset or liability. Expressing the value of privacy for a company will vary from business to business, but the value generally includes compliance with laws and regulations and has a reputation of trustworthiness.

Third, to reinforce training, a company should seek to have one or more privacy professionals in every business unit.[67] These individuals are tasked with ensuring a business's privacy policies are followed throughout the firm beyond any annual training.

Fourth, depending on the company's size and budget, emphasis on building and documenting compliance programs may lead to creating a team of privacy professionals.[68] After assembling its team, the group should "discuss and develop an action plan to mitigate . . . [any] identified risks."[69] The action plan should contain the following five components: administrative safeguards, physical safeguards, technical safeguards, organizational standards, and policies and procedures.[70] Specifically, healthcare firms should "[t]ake advantage of the flexibility that the HIPAA Security Rule provides, which allows [a company] to achieve compliance while taking into account the characteristics of [its] organization and its environment."[71] Moving from

[64] IPC Technical Report, Privacy by Design Solutions for Biometric One-to-Many Identification Systems, INFO. & PRIV. COMM'R ONT. 4 (Jun. 2014), https://www.ipc.on.ca/wp-content/uploads/2014/06/pbd-solutions-biometric.pdf. [https://perma.cc/TMU7-6SR9]; *see also* Bolinger, *supra* note 58.

[65] Bolinger, *supra* note 58.

[66] *Id.*

[67] *See Everything you need to know about the GDPR Data Protection Officer (DPO)*, GDPR.EU, https://gdpr.eu/data-protection-officer/ [https://perma.cc/4KAF-FH22].

[68] *See* Bolinger, *supra* note 58 (discussing how current employees at the company may have some expertise or interest in privacy).

[69] *See* Department of Health & Human Services, *Guide to Privacy and Security of Electronic Health Information*, https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf [https://perma.cc/RC6R-UR85].

[70] *See id.* (containing a detailed breakdown of each component and what they should contain).

[71] *Id.*

discussion to implementation of an action plan demonstrates that the privacy plan is maturing.

Finally, a company should continue to "monitor, audit, and update security on an ongoing basis."[72] Healthcare companies should remain cognizant of HIPAA's Security Rule requirements that they have audit controls in place and the ability to conduct an audit. HIPAA uses the term "audit" in two ways. The first way HIPAA uses audit is to describe "what [a company] do[es] to monitor the adequacy and effectiveness of [its] security infrastructure and make needed changes."[73] In the second context, an audit refers to an effort to examine what happened after the fact (often of a security incident).[74]

D. AI Laws & Regulations

Like with its privacy laws and regulations, the United States lacks comprehensive laws and regulations surrounding the use of AI.[75] Although there is no comprehensive federal regulation at this time, it is highly anticipated that the FTC will soon regulate the AI landscape.[76] On April 19, 2021, the FTC foreshadowed the next steps in a blog post.[77] The FTC stated concerns with AI, as "neutral' technology can produce troubling outcomes—including discrimination by race or other legally protected classes."[78] The FTC announced its AI regulations would be premised on its authority under Section 5 of the FTC Act, the Fair Credit Reporting Act, and the Equal Credit Opportunity Reporting Act.[79] Additionally, on December 10, 2021, in an advanced notice of proposed rulemaking, the FTC stated they were "considering initiating a rulemaking under section 18 of the FTC Act to curb lax security practices, limit privacy abuses, and ensure that algorithmic decision-making does

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] Martin Pereyra, *The State of Artificial Intelligence in the United States*, FORDHAM J. OF CORP. & FIN. L. (Nov. 29, 2021), https://news.law.fordham.edu/jcfl/2021/11/29/the-state-of-artificial-intelligence-in-the-united-states/ [https://perma.cc/CE8A-AVM9].

[76] *Janis Kestenbaum Quoted in IAPP: The Privacy Advisor—FTC Takes Steps Toward Privacy, AI Rulemaking*, PERKINS COIE (Dec. 13, 2021), https://www.perkinscoie.com/en/news-insights/janis-kestenbaum-quoted-in-international-association-of-privacy-professionalsftc-takes-steps-toward-privacy-ai-rulemaking.html [https://perma.cc/H2UN-BQXZ].

[77] Elisa Jilson, *Aiming for truth, fairness, and equity in your company's use of AI*, FTC (Apr. 19, 2021), https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai [https://perma.cc/FF6K-PRDN].

[78] *Id.*

[79] *Id.*

not result in unlawful discrimination."[80] Most recently, in its latest report to Congress, the FTC recommended "development of [carefully crafted] legal frameworks that would help ensure . . . use of AI does not itself cause harm."[81]

Alongside the FTC, the FDA has signaled potential regulation of AI.[82] On January 12, 2021, the FDA released the *Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan* (Action Plan).[83] There, the FDA outlined "five actions that the [agency] intends to take," which are focused on: (1) developing a regulatory framework for AI/ML-based SaMD; (2) supporting good machine learning practices development; (3) fostering a patient-centered approach incorporating transparency; (4) developing regulatory science methods related to algorithm bias and robustness; and (5) advancing real-world performance.[84] As federal regulators move toward promulgating AI-related regulations, the National Institute of Standards and Technology (NIST), a non-regulatory agency within the Department of Commerce dedicated towards advancing measurement science, standards, and technology, has taken steps towards producing a "comprehensive socio-technical approach to testing, evaluation, verification, and validation of AI systems" to help develop guidance for best-practices and promote positive outcomes for society through the use of AI.[85]

[80] FTC, *Proposed Trade Regulation Rule on Commercial Surveillance (Fall 2021)*, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=3084-AB69; Clayton Northouse, Lauren Kitces, & Alexandra Mushka, *FTC Announces it May Pursue Rulemaking to Combat Discrimination in AI*, DATA MATTERS (Dec. 28, 2021), https://datamatters.sidley.com/ftc-announces-it-may-pursue-rulemaking-to-combat-discrimination-in-ai [https://perma.cc/87H3-FFW4].

[81] FTC, *Combatting Online Harms through Innovation–Report to Congress* (June 16, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Combatting%20Online%20Harms%20Through%20Innovation%3B%20Federal%20Trade%20Commission%20Report%20to%20Congress.pdf.

[82] Press Release, U.S. Food & Drug Admin., FDA Releases Artificial Intelligence/Machine Learning Action Plan (Jan. 12, 2021), https://www.fda.gov/news-events/press-announcements/fda-releases-artificial-intelligencemachine-learning-action-plan; LaDale K. George, Elijah Roden, *FDA Announces Action Plan for Oversight of AI/ML in Medical Devices*, PERKINS COIE (Jan. 27, 2021), https://www.perkinscoie.com/en/news-insights/fda-announces-action-plan-for-oversight-of-aiml-in-medical-devices.html [https://perma.cc/VE7X-W7SM].

[83] *See* Press Release, *supra* note 82.

[84] *Id.*

[85] *Workshop on Mitigating AI Bias in Context*, NAT'L Institute of Standards and Technology (Aug. 18, 2022), https://www.nccoe.nist.gov/get-involved/attend-events/workshop-mitigating-ai-bias-context/overview; *see also Towards a Standard for Identifying and Managing Bias in Artificial Intelligence,* NAT'L Institute of Standards and Technology (March 2022), https://nvlpubs.nist.gov/

Some states have enacted AI-related legislation.[86] California is a pioneer with its California Privacy Rights Act (CPRA), the first state legislation to include restrictions on dark patterns[87], including as applied to AI.[88] These regulations encouraged subsequent AI regulations, such as (1) Colorado and Washington introducing legislation on dark patterns;[89] (2) Congress introducing the *Deceptive Experiences to Online Users Reduction (DETOUR) Act*;[90] and (3) the FTC publishing a request for public comment on dark patterns, which is set to close on August 2, 2022.[91]

The European Union (EU) addresses this issue directly with the Digital Services Act (DSA).[92] The DSA—one of two laws with the Digital Markets

nistpubs/SpecialPublications/NIST.SP.1270.pdf; *see also Dioptra 0.0.0 documentation*, NAT'L Institute of Standards and Technology (2022), https://pages.nist.gov/dioptra/.

[86] *See State-by-State Artificial Intelligence Legislation Tracker*, U.S. CHAMBER OF COM. (Apr. 06, 2022), https://www.uschamber.com/technology/state-by-state-artificial-intelligence-legislation-tracker*; see also Legislation Related to Artificial Intelligence*, NAT'L CONF. OF STATE LEGIS. (Jan. 5, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx.

[87] "Dark Patterns" is a phrase "used to describe a range of potentially manipulative user interface designs used on websites and mobile apps." *Bringing Dark Patterns to Light: An FTC Workshop*, FTC (Apr. 29, 2021), https://www.ftc.gov/news-events/events-calendar/bringing-dark-patterns-light-ftc-workshop [https://perma.cc/A7MU-UHCR].

[88] *CPRA's provisions on dark patterns a first for US law*, IAPP (Feb. 1, 2021), https://iapp.org/news/a/cpras-provisions-on-dark-patterns-a-first-for-us-law/ [https://perma.cc/RJ4H-QNSA]; *see also* Brian H. Lam, *Beware Dark Patterns - What are They and What Should Your Business Do About Them?*, 12 NAT'L L. REV. (Apr. 2, 2021), https://www.natlawreview.com/article/beware-dark-patterns-what-are-they-and-what-should-your-business-do-about-them.

[89] Catherine Zhu, *Dark patterns — a new frontier in privacy regulation*, REUTERS (Jul. 29, 2021, 10:56 AM), https://www.reuters.com/legal/legalindustry/dark-patterns-new-frontier-privacy-regulation-2021-07-29/ [https://perma.cc/E2D4-YE7M].

[90] *Lawmakers Reintroduce Bipartisan Bicameral Legislation to Ban Manipulative 'Dark Patterns'*, MARK. R. WARNER (Dec. 8, 2021), https://www.warner.senate.gov/public/index.cfm/2021/12/lawmakers-reintroduce-bipartisan-bicameral-legislation-to-ban-manipulative-dark-patterns [https://perma.cc/JGD5-MWAU].

[91] Lesley Fair, *FTC calls for a reboot on business guidance about digital advertising*, FTC (Jun. 3, 2022), https://www.ftc.gov/business-guidance/blog/2022/06/ftc-calls-reboot-business-guidance-about-digital-advertising.

[92] *The Digital Services Act Package*, EUROPEAN COMM'N, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package [https://perma.cc/X5UN-HJMF].

Act that makes up the EU's Digital Services Packet—was adopted by EU Parliament in July 2022.[93] Once effective, the DSA aims to improve "the mechanisms for the removal of illegal content and for the effective protection of users' fundamental rights online" and create "a stronger public oversight of online platforms."[94] This includes implementing different measures and bans which could impact the use of AI, specifically black box algorithms.[95] In addition to the DSA, the EU may also soon regulate AI through a proposal referred to as the European Artificial Intelligence Act (EU AI Act).[96]

E. Artificial Intelligence & Algorithmic Bias

While AI utilization in medical devices has the potential to improve patient outcomes, it can also, just as the humans wielding it, suffer from bias. Algorithmic bias was first defined by Trishan Panch and Heather Mattie as "the application of an algorithm that compounds existing inequities in socioeconomic status, race, ethnic background, religion, gender, disability, or sex-

[93] *Id.*

[94] *The Digital Services Act: Ensuring a Safe and Accountable Online Environment*, European Comim'n, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en [https://perma.cc/D88U-BVAY].

[95] *Id.*; *Pulling Back the Curtain on the 'Black Box': How the Digital Services Act Will Legislate Algorithmic Auditing*, Glob. Network Initiative (Jul. 22, 2020), https://medium.com/global-network-initiative-collection/pulling-back-the-curtain-on-the-black-box-the-dsa-and-algorithmic-auditing-by-ilse-heine-4b628840bb3b [https://perma.cc/WY7R-S6KR].

[96] Marc S. Martin, Charlyn L. Ho, & Kyle R. Canavera*, Europe Seeks to Tame Artificial Intelligence With the World's First Comprehensive Regulation*, Perkins Coie (Apr. 28, 2021), https://www.perkinscoie.com/en/news-insights/europe-seeks-to-tame-artificial-intelligence-with-the-worlds-first-comprehensive-regulation.html [https://perma.cc/YE6B-27T2]; *see* Mauritz Kop, *EU Artificial Intelligence Act: The European Approach to AI*, Transatlantic Antitrust & IPR Dev. (2021); *see also* Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, (2021/0106) (COD) COM (2021) 206 Final, (Apr. 21, 2021), https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF. In an April 21, 2021, proposal, the EU called for regulation "laying down harmonized rules" on AI. The EU AI Act proposes regulating AI through a four-step framework which focuses on: (1) "ensur[ing] that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values"; (2) "ensuring legal certainty to facilitate investment and innovation in AI"; (3) "enhancing governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems"; and (4) "facilitat[ing] the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation."

ual orientation and amplifies inequities in health systems."[97] When present in the algorithm, this bias can lead to inaccurate predictions of cardiovascular diseases.[98] For example, among minority ethnic groups, because many existing data samples are not representative of the overall population.[99] Algorithmic bias is exacerbated by collecting data from populations that may not properly reflect the full set of users.[100] Ensuring that a company collecting data is following proper data collection and processing methods and identifying any instances of bias or potential biases and correcting them may drastically reduce algorithmic bias.[101]

The House Commerce Committee is currently taking action to limit algorithmic bias.[102] In a recent 53-2 vote, the committee advanced the American Data Privacy and Protection Act (ADPPA), which would, among other privacy directives, "clamp[ ] down on algorithmic bias."[103] If the act passes Congress, covered entities and service providers will be prohibited "from collecting, processing, or transferring covered data 'in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services based on race, color, religion, national origin, sex, or disability."[104] Additionally, covered entities would be required to perform impact assessments and design evaluations to ensure that their algorithms are not biased.[105]

[97] *See* Katherine J. Igoe, *Algorithmic Bias in Health Care Exacerbates Social Inequities — How to Prevent It*, HARV. T.H. CHAN SCH. OF PUB. HEALTH, https://www.hsph.harvard.edu/ecpe/how-to-prevent-algorithmic-bias-in-health-care/ [https://perma.cc/C9YW-M3S5]; *see also* Trishan Panch Heather Mattie, Rifat Atun, *Artificial Intelligence and Algorithmic Bias: Implications for Health Systems*, 9 J GLOB HEALTH (2019).

[98] *See* Igoe, *supra* note 97. Where the prediction of cardiovascular diseases amongst Caucasian patients was more accurate than African American patients in one AI study. Caucasians made up about 80 percent of collected data, and this is the case with a majority of data samples. This disproportionality can lead to inaccurate predictions of any kind for minority groups.

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] Allison Grande, *Bills Boosting Kids' Online Privacy Rights Head To Full Senate*, L. 360 (Jul. 27, 2022), https://www.law360.com/cybersecurity-privacy/articles/1515354/bills-boosting-kids-online-privacy-rights-head-to-full-senate?nl_pk=566dc82a-51d3-4ba0-a5d7-9538735735c7&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy&utm_content=2022-07-28?copied=1 [https://perma.cc/HT2G-UQZM].

[103] *Id.*

[104] Jane Blaney, et al., *Artificial Intelligence Briefing: Feds Take Aim at Algorithmic Bias*, JD SUPRA (Jul. 1, 2022), https://www.jdsupra.com/legalnews/artificial-intelligence-briefing-feds-8436960/ [https://perma.cc/UZ8U-PUAB].

[105] *Id.*

Medical device and technology companies, like Oculogica, that utilize AI and ML in their products must grapple with the realities of using big data sets.

Additionally, the large amounts of data required to train an algorithm circle right back to the data security and privacy concerns discussed above. AI algorithms often require access to large datasets, and this collection and transfer of data present challenges that are new to many healthcare companies.[106] The Cloud Security Alliance (CSA), an organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment, suggests that "organizations combat AI data security concerns by ensuring solid access controls and multi-factor authentication, as well as implementing endpoint security and anomaly detection technologies."[107]

By understanding the causes of algorithmic biases, companies can combat them.[108] Any company can do this by ensuring that their algorithms are properly developed to avoid bias.[109] Additionally, if a company notices any bias in their algorithms, immediately recalling them will help mitigate harm to patients. As Zac Stewart Rogers, a supply chain management professor from Colorado State University, explained, "[w]ith coding, a lot of times you just build the new software on top of the old software."[110] Thus, any new software will also be contaminated if the underlying code is biased.[111] The harmful effects of ignoring or not addressing algorithmic bias can manifest in multiple ways. For example, crime prediction algorithms unfairly target "Black and Latino people for crimes they did not commit or facial recognition systems that do not reliably and accurately identify people of color."[112]

Ultimately, there are at least three steps a company should take to mitigate biases in machine-learning algorithms. First, "users of machine-learning algorithms need to understand an algorithm's shortcomings and refrain from

[106] Jill McKeon, *AI in Healthcare Presents Need for Security, Privacy Standards*, Health IT Sec. (Feb. 17, 2022), https://healthitsecurity.com/features/ai-in-healthcare-presents-need-for-security-privacy-standards.

[107] *Id.*

[108] Pranshu Verma, *These Robots Were Trained on AI. They Became Racist and Sexist.*, The Wash. Post (Jul. 16, 2022), https://www.washingtonpost.com/technology/2022/07/16/racist-robots-ai/.

[109] Emily Bembeneck, Rebecca Nissan, & Ziad Obermeyer, *To Stop Algorithmic Bias, We First Have to Define It*, Brookings (Oct. 21, 2021), https://www.brookings.edu/research/to-stop-algorithmic-bias-we-first-have-to-define-it/ [https://perma.cc/4FY2-BMSX].

[110] Verma, *supra* note 108.

[111] *Id.*

[112] *Id.*

asking questions whose answers will be invalidated by algorithmic bias."[113] Second, "data scientists developing the algorithms must shape data samples in such a way that biases are minimized."[114] Third, the user and developers of the algorithm should understand the trade-offs involved in using an algorithm.[115] Algorithms "offer speed and convenience, while manually crafted models, such as decision trees or logistic regression—or for that matter even human decision making—are approaches that have more flexibility and transparency."[116] Thus, although AI and machine learning are rapidly growing fields, developers should remember that AI is "as prone to bias as the real thing it emulates."[117]

3. CASE STUDY: OCULOGICA'S EYEBOX

Oculogica, like any start-up medical device company also feels the constraints of limited budget and competing resources. However, as shared by its CEO Dr. Rosina Samadani, the company has prioritized privacy and data security. And, consistent with privacy by design principles, they have baked privacy and data security into many aspects of the business. Moreover, the company takes algorithmic biases seriously and has identified weak points in data sets. Further, Oculogica is actively working to expand the pool of data participants, particularly to those of minorities and people of color, to address any potential algorithmic bias in their data sets.

On privacy, the company has focused on 21 CFR Part 11 compliance, implementing the necessary controls, including audits, data encryption, access-controls, and system validations. Dr. Rosina Samadani explained that the company has invested significant time, money, and effort to train their staff in the CITI. Oculogica understands that many of these privacy-focused initiatives are required by law, but also believe the initiatives are necessary to build trust with their target audience—healthcare providers—and the patients they serve.

On security, even in the start-up phase, Oculogica has expended significant time and resources to ensure that company's cybersecurity practices are comparable to those of larger and more established companies. Oculogica has completed penetration testing of its systems, appointed a Quality System Specialist to assume privacy officer duties, and regularly complies with all new FDA cybersecurity requirements. Dr. Rosina Samadani explained that with submissions to the FDA, Oculogica is required to record their informa-

[113] Tobias Baer and Vishnu Kamalnath, *Controlling machine-learning algorithms and their biases*, McKinsey & Co. (Nov. 10, 2017), https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/controlling-machine-learning-algorithms-and-their-biases [https://perma.cc/FH3T-7WYV].

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] *Id.*

tion security practices in significant detail as part of the review and approval processes. Oculogica currently has 4 FDA clearances, 3 of which were submitted post the FDA draft cybersecurity guidelines.

Where Oculogica aims to set itself apart is their acute focus on PbD and addressing algorithmic bias. The company believes that the technology behind EyeBOX can be used for far more than just diagnosing concussions, despite currently only having FDA clearance for that indication. Oculogica also plans to further its use of AI/ML to improve and expand the utility of its device to other diagnoses that rely on measures of pupil characteristics. But, how does a company that relies on an algorithm making assumptions from data combat the "black box" and unintended algorithmic biases in delivering healthcare?

Algorithms such as those used in Oculogica's EyeBOX are used as "a screening tool, in part to alert primary care doctors to high-risk patients" in brain injury cases.[118] If algorithmic bias occurs during screening, there is a possibility that a false negative test or a false positive test would be produced.[119]

Oculogica aims to go beyond the steps described in Part 2.D. Not only does Oculogica try to shape data samples in ways that minimize biases, the company also actively solicits individuals of underrepresented groups to participate in their studies.[120] Additionally, with their EyeBOX in the offices of many physicians now, Oculogica is working to collect data from individuals that received medical attention, not just participants of studies, i.e., "real life use". With these efforts to widen their dataset, Oculogica seeks to assure that their algorithms are less biased and more accurate by being representative of the actual population.

It may not be possible, though, to completely eliminate algorithmic bias. Abeba Birhane, a senior fellow at the Mozilla Foundation who studies racial stereotypes in language models, explained that "it's nearly impossible to have artificial intelligence use data sets that aren't biased, but that doesn't mean companies should give up."[121] Birhane added that "companies must audit the algorithms they use, and diagnose the ways they exhibit flawed behavior, creating ways to diagnose and improve those issues."[122] With the rapid use and adoption of AI and robots in various facets of the world, the problem of bias will only worsen if companies do not make changes. If more

[118] Ziad Obermeyer, Brian Powers, Christine Vogeli, & Sendhil Mullainathan, *Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations*, 366 Sci. 395, 447–453 (2019).

[119] *De Novo Classification Request*, *supra* note 9.

[120] Dr. Rosina Samadani has shared about Oculogica's ongoing collaborations to recruit individuals belonging to minority races and ethnicities to participate in their studies, which they believe were underrepresented in their research.

[121] Baer, *supra* note 113.

[122] Baer, *supra* note 113.

companies invest time and resources into unpacking and solving for algorithmic biases, products and patient care will benefit significantly.

CONCLUSION

Considering how quickly the AI/ML space has evolved, it is no surprise that both legislators and regulators are trying to adapt and scrutinize these new technologies. The FTC and FDA have stepped up their guidance, rulemaking, and enforcement activities, particularly in the healthcare space. However, as the United States continues to lag behind in regulating modern advances in AI/ML developments, challenges are created for organizations with scarce resources, compounded by the constantly shifting legal landscape.

Ultimately, regulators seek to protect the public well-being. Considering the harm that can result from the improper use of patient data or the biases (including algorithmic) that exist in the medical field, addressing privacy and security concerns associated with personal data, and mitigating algorithmic bias are motivated by the same goals. For a healthcare company, keeping patient health and well-being as a primary goal can help provide an acknowledgment of the regulator's intent. This can be accomplished by: (1) building a privacy and compliance-minded culture that emphasizes privacy and algorithmic fairness early in development and promotes PbD principles; (2) maintaining a positive intent and consistently assessing privacy and data security compliance; (3) being transparent with employees, regulators, customers, patients, and data subjects about data use, collection, retention, and deletion; and (4) making true efforts and investment in algorithmic fairness by continual evaluation of the algorithms and addressing any real or potential bias resulting from the underlying data set(s) and model(s).

Even where resources are scarce and personnel are stretched, firms (start-ups, in particular) can and should be privacy-minded. Staying compliant with existing laws and getting ahead on issues of algorithmic fairness will place certain start-ups ahead of the pack as these issues become more pressing to regulators, consumers, and the general public.