Following Footsteps: How Federal District Court Jurisprudence Protects Health Data in the Workplace

ABSTRACT

With the growing popularity of fitness tracking technology, employers have started to provide their employees with fitness tracking devices in order to obtain a subsidy on employer group health plans. Access to this data creates an opportunity to abuse the data by using it when making employment decisions. This Note analyzes how the current legal framework does not adequately protect the data and employees. The solution suggests using a recent case to provide the Equal Employment Opportunity Commission with authority to regulate employers’ use of the health data until adequate privacy and data security laws can address the problem.

TABLE OF CONTENTS

I. CORPORATE FITNESS TRACKING DEVELOPMENT .................... 323
II. PROBLEMS ARISING FROM CORPORATE FITNESS TRACKING ..... 326
    A. Privacy Concerns ................................................................. 326
    B. Adverse Employment Actions ................................................. 330
III. CURRENT SOLUTIONS FOR PROTECTING DATA AND THEIR INADEQUACY ................................................................. 333
    A. Health Insurance Portability and Accountability Act ............ 334
    B. Computer Fraud and Abuse Act ............................................. 335
    C. Americans with Disabilities Act .......................................... 336
IV. PROPOSED SOLUTIONS ............................................................ 343
    A. Follow Chief Judge Griesbach by Giving Deference ............... 344
    B. Suggested Changes to Current Regulations .............................. 344
        1. Bolster Confidentiality ...................................................... 345
        2. Eliminate the Voluntary Examination Loophole ................. 347
    C. Insignificance of Eliminating Chevron Deference .................. 348
V. CONCLUSION ............................................................................ 349
In 2010, the Equal Employment Opportunity Commission (EEOC) filed a claim on behalf of Lisa Harrison’s estate, alleging that her employer discriminated against her based on her weight. In a case that has recently gone to settlement negotiations, Edward Bess claimed he was fired because his employer found that he had high blood pressure. Moreover, in 2007, a Massachusetts lawn and garden company fired Scott Rodrigues because his drug test showed positive results for nicotine. The company had an antismoking policy, and Rodrigues did not smoke at work; nevertheless, he was fired because of his off-duty legal activity. Employment lawyers refer to these actions as “lifestyle discrimination,” which springs as a result of an employer’s interest in preempting health insurance expenses.

Employers bear massive health insurance costs by acting as the group insurer for their employees. Employers therefore have financial incentives to hire and retain healthy employees, both for lower health insurance costs and higher productivity. Therefore, employees that show signs of unhealthy habits can pose a risk to corporate success. While employers may be subject to liability for firing employees based on unhealthy lifestyles, they can probably avoid liability by articulating a nondiscriminatory reason for a firing or promotional decision while keeping health reasons implicit or quiet. As Gary Phelan, an employment lawyer and author of the Disability Discrimination in the Workplace treatise said, “What sounds pretty outrageous doesn’t necessarily make it illegal[;] . . . the next thing they’ll be testing for is cholesterol. Or they won’t hire you because both of your parents died of heart attacks when they were 45, or if you skydive.”

---

4. Id.
5. Id.
7. See id.
8. See id.
9. See id. (stating that employers have a wide array of tools they can use to fire employees, such as simply saying that their quality of work is low).
Because employers have a strong interest in hiring and retaining healthy employees, access to more health information poses a risk to employees and their job opportunities. Some health insurance companies offer employers insurance subsidies if they provide their employees with fitness-tracking devices. However, tracking devices create an additional avenue to health data and could therefore threaten employees’ careers if employers explicitly or implicitly motivate decisions based on health statistics.

While employees may not have an issue with their employers receiving subsidized health insurance by tracking employee fitness, there are underlying concerns that employees must account for. Primary concerns include privacy, data security, and adverse employment actions that stem from employers’ increased access to health information. For example, fitness trackers provide insight into employees’ lives that those individuals may not want others to access. While employees may be comfortable with insurance companies analyzing anonymous statistics during valuation, the same employees may not like their employers’ management accessing that same information. Further, fitness trackers are subject to security breaches and data leaks that expose user information and data to outside parties.

While privacy concerns are significant, perhaps the most crucial concern is the effect that fitness trackers can have on employees’ job security and treatment in the workplace. When companies have access to employees’ health data, they could consider the data when making employment decisions. For example, one employee could receive a promotion over another because the employer feels assured that the promoted employee will be able to

12. See, e.g., Julie Bort, This Company Saved a Lot of Money by Tracking Their Employees with Fitbits, BUS. INSIDER (July 7, 2014, 8:59 PM), http://www.businessinsider.com/company-saved-money-with-fitbits-2014-7 [https://perma.cc/2PGM-MZQ8]; see also Parmy Olson, More Bosses Expected to Track Their Staff Through Wearables in the Next 5 Years, FORBES (June 1, 2015, 7:47 AM), http://www.forbes.com/sites/parmyolson/2015/06/01/wearables-employee-tracking/#4a7c1c5eeec9 [https://perma.cc/YZ23-CE88].
15. See Olson, supra note 12; see also Caplan, supra note 6; Dahl, supra note 3.
work longer without encountering health threats. These employment actions can extend further to hiring and firing decisions as well.  

With wearable devices becoming more prevalent in the workplace, solutions to privacy and employment concerns are necessary. Some scholarly suggestions aim to solve both problems by restricting access to health data and subjecting wearable devices to privacy and data security laws. However, considering that job security is a top concern for employees, and protection from existing privacy and data security laws is inadequate at best, finding a solution to adverse employment actions is necessary before resolving the problem entirely. A readily available solution to employment concerns—rooted in existing case law and agency regulation—already exists, avoiding a complicated and ultimately ineffective solution to both privacy and employment concerns.

This Note suggests using Chief Judge William C. Griesbach’s analysis of the Americans with Disabilities Act (ADA) in EEOC v. Orion Energy Systems, Inc.—which leaves the EEOC with power to regulate the employment issues faced by fitness tracker usage—in order to halt adverse employment actions and allow time for effective privacy and data security solutions to develop. Part I reviews the general landscape of fitness tracking and shows how corporations can use fitness tracking in their corporate wellness programs for various advantages. Part II highlights the issues that corporate fitness tracking presents and suggests that, at the moment, job security concerns are more critical than privacy and data security concerns. Part III reviews proposed solutions to the issues established in Part II and also shows how such solutions fail to adequately address employees’ main concerns. Part IV sets forth the proposed solution by

utilizing Chief Judge Griesbach’s *Orion* opinion and discusses how the EEOC can regulate the largest concern arising from corporate fitness tracking—adverse employment actions. Part V briefly concludes by recognizing that this solution solves the employment concerns rather than the privacy and data security concerns but advocates that this is the most efficient, sufficient, and essential solution before reaching a complete solution to the privacy and data security concerns.

**I. CORPORATE FITNESS TRACKING DEVELOPMENT**

Between April 2013 and March 2014, Americans purchased 3.3 million wearable devices (or “wearables”) designed specifically for fitness tracking. The most popular fitness tracker, Fitbit, accounted for approximately two-thirds of fitness tracker sales in 2014. Other fitness trackers implement similar software to that of Fitbit, which can track number of steps per day, calories burned, heart rate, and sleep data. Fitbit maintains a strong percentage of the market share, but other brands of fitness trackers are also effective and accessible.

The fitness tracker market is declining, but the number of wearables that contain fitness tracking technology, such as smartwatches, remains high. Other wearable technologies contain the same fitness tracking software as Fitbits but simply subsume that software into a universal wearable device. Apple has even taken steps to file a patent for headphones—the updated version of the Apple AirPods—that could include technology to monitor electrical heart activity, cardiac output, and heart rate, for starters.

---

22. See *Orion*, 208 F. Supp. 3d at 996, 1002.
24. Id.
26. See Danova, supra note 23.
Particularly, the number of wearables provided by employers is expected to increase to 27.5 million by 2020, as opposed to the 166,000 provided in 2013. Therefore, usage of fitness tracking technology continues to prevail in personal and employment capacities.

Companies primarily use fitness tracking technology in order to receive more favorable health insurance policies. The standard health insurance policy may not consider the well-being of a specific employee. Rather, it may just group the employees into a large policy that is customary for similar companies. Health insurance providers may track the health of key executives or board members without considering the health of lower-level employees as heavily. However, fitness trackers provide employers with the ability to show health insurers that their employees are healthy and that the company deserves a favorable health insurance policy. Instead of receiving standard health insurance treatment, companies using fitness tracking have the opportunity to show insurers that they deserve cheaper insurance policies. For example, employees at British Petroleum were eligible for a discount if they reached their step goals during the company’s Million Step Challenge through Fitbit. Additionally, Appirio, a worker and customer experience technology company, received a $300,000 discount on its $5 million insurance costs by sharing employee health data with its insurer.

Aside from insurance advantages, companies also believe that fitness tracking can increase workplace production and efficiency. Exercising and maintaining good health can lead to lower stress levels and increase ability to absorb and retain information. Correspondingly, employees who sleep the proper amount of hours are

30. Olson, supra note 12.
31. See Danova, supra note 23; Olson, supra note 12.
33. See id.
34. Id.
35. See id.
36. See id.
37. Id. at 15.
41. Id.
more alert at work. While individuals usually want to reap the benefits of being healthy, it is clear that businesses also stand to benefit from healthy employees. Therefore, fitness tracking could increase companies’ productivity in addition to providing the companies with an opportunity for reduced health insurance costs.

Studies show various additional benefits, for both the employer and employee, of tracking fitness and having a general corporate wellness program. Fitness trackers may be a part of a company’s overall corporate wellness program. These programs, altogether, prove valuable and desirable to employees while providing the aforementioned benefits to employers. Wellness programs reduce stress in the workplace more than company get-togethers and attract, engage, and retain more employees. Data from the Health Enhancement Research Organization even suggest that companies with corporate wellness programs substantially outperform the S&P 500.

While corporate wellness programs provide numerous benefits for the employer, individuals are familiar with the benefits that can come from fitness tracking. In 2015, insurance company John Hancock began offering insurance advantages to individuals who agree to provide fitness and activity data. The structure of the insurance program is similar to that of the corporate insurance structure—individuals receive free fitness trackers and exchange their data for lower life insurance premiums and other discounts. These programs also encourage fitness awareness and maintaining an active lifestyle, similar to the corporate fitness tracking programs. The substantial difference is that individuals participating in personal programs opt into the program for personal fiscal and health benefits, without the risk of employment decisions against them. Individual insurance programs present privacy and data security concerns from

---

43. See Martin, supra note 40.
44. Id.
45. See id.
46. Id.
47. Id.
48. Id. Consider that this finding may be more correlation than causation.
50. Id.
51. Id.
security breaches and data leaks, similar to privacy and data security concerns in corporate programs. Altogether, the ultimate beneficiary of the corporate program is the company, while the corporate program subjects employees to job security threats that they do not encounter when participating in an individualized life insurance program. However, group healthcare plans are often cheaper for individuals in the group plan than if they insured themselves.

The advantages, in both an individual and corporate program, can be widespread and beneficial to both the insurer and insured. While individuals may understand the advantages and reasoning behind incorporating fitness tracking into a corporate insurance program, the risks associated with the corporate programs demand solutions.

II. PROBLEMS ARISING FROM CORPORATE FITNESS TRACKING

While a productive workplace and favorable health insurance policy are desirable, tracking fitness to attain such corporate advantages is problematic. The two main issues that arise when companies track employees’ fitness are employee concerns over privacy of the data and adverse employment actions based on data results.

A. Privacy Concerns

Using data-collecting technology comes with inherent risks of privacy and data security of the information. Emerging technologies collect user information for various purposes, ranging from simple data collection (as in fitness trackers) to tracking user preferences and tendencies for a more personal, unique user experience. Data collection can be an advantage both to users and technology creators. Users can have improved experiences with the technology, while


55. See id.
creators keep their consumers pleased and gain access to information indicating consumer preferences. Therefore, data collection will not stop in the future, as it has become a staple in modern and emerging technology.

While individual owners might worry about third parties gaining access to their health data, privacy concerns are different for employees using fitness trackers. Ideally, employees use the fitness trackers knowing that their employer may use the data for company health insurance purposes. Employee knowledge of the employers’ intent eliminates some of employees’ main concerns about companies gaining access to health data. However, employers could make misrepresentations about the prospective use of health data, reviving privacy concerns.

Typically, when employers collect health data from employees, they assure employees that the data will be kept anonymous. A common method for maintaining confidentiality of employee health data is for the company to hire a third-party vendor that collects and manages the data. For example, in EEOC v. Orion Energy Sys., Inc., Orion Energy Systems, Inc. (Orion) required employees enrolled in...
Orion’s insurance plan to complete a health risk assessment (HRA) or pay their entire monthly premium.\textsuperscript{61} The HRA was similar to a physical, in that it contained a health history questionnaire and collected blood pressure, height, weight, body circumference, and blood analysis.\textsuperscript{62} Orion did not receive the personal information from the HRA; instead, third party Holy Family Memorial collected the information and sent it to Clinical Reference Lab.\textsuperscript{63} Thereafter, another company, Healics, managed the data and created an aggregate collection of the health information.\textsuperscript{64} Only after Healics compiled the data did Orion gain access to it.\textsuperscript{65} Orion had access to the anonymous, aggregated data and could use the data to see the percentage of people in its insurance plan who had certain health risks.\textsuperscript{66} The HRA form filled out by employees stated that the third-party vendors who handled the information were the only companies with access to the individual health data and that the companies considered the employees’ health data as “Protected Health Information” under the Health Insurance Portability and Accountability Act (HIPAA).\textsuperscript{67}

Another company, Flambeau, Inc., used a similar aggregate data collection method that identified health risks and conditions prevalent among the company’s employees (although not individualized to single out particular employees).\textsuperscript{68} Companies use this aggregation method so they can set premiums, adjust copays, and assess the need for different types of insurance, wellness initiatives, and changes\textsuperscript{69} in the workplace.\textsuperscript{70} Facially, collecting health data can save money for both the company and the employees.\textsuperscript{71} Even 40 percent employee participation can lead to proof that employees at the company are healthy, or becoming healthier, due to participation in

\textsuperscript{61.} Id. at 992.
\textsuperscript{62.} Id.
\textsuperscript{63.} Id.
\textsuperscript{64.} Id.
\textsuperscript{65.} Id. at 992–93.
\textsuperscript{66.} Id. at 993.
\textsuperscript{67.} Id.
\textsuperscript{68.} Equal Emp’t Opportunity Comm’n v. Flambeau, Inc., 131 F. Supp. 3d 849, 852 (W.D. Wis. 2015).
\textsuperscript{69.} Id. Examples of such changes could be modifying vending machine options and sponsoring weight loss competitions. See id.
\textsuperscript{70.} Id.
\textsuperscript{71.} See Brown, supra note 16, at 15–16.
the health program.\textsuperscript{72} This proof can convince health insurance companies to cut costs from the employer’s insurance.\textsuperscript{73}

Additionally, handling data collected through tracking devices may present privacy issues even greater than those presented by the HRA data Orion collected from its employees.\textsuperscript{74} New tracking devices can record time spent at desks, enthusiasm during conversations, and behavioral data when employees are near each other, along with the typical fitness statistics for which fitness trackers were originally created.\textsuperscript{75} These tracking devices are proven to increase workforce productivity, but they also come with their own privacy concerns.\textsuperscript{76} However, when companies require employees to wear tracking devices that record such activities, employees typically know how and why such data are being used.\textsuperscript{77} For example, employees wearing Hitachi’s Business Microscope know that the company requiring them to wear the device will make use of the data recorded from the device.\textsuperscript{78} Companies considering implementing such a program merely balance whether the company wants to utilize the devices for the benefit of productivity and the risk of disgruntled employees concerned about privacy. The issue with tracking devices arises, however, when fitness data intended for use in a specific manner is used in another. Typically, employers inform employees that their data will be used anonymously in an aggregate format that does not identify any individual health risks or concerns.\textsuperscript{79} Nevertheless, privacy concerns arise when employees become skeptical that the data collected and managed by third parties will become accessible to employers.\textsuperscript{80}

Therefore, it is not the data security of information at the third-party level, but the data leakage to employers and other parties that concerns employees. Employees understand that tracking health data can help their company and, in turn, help employees save money. The concern over privacy sprouts from employee concerns over health data being used for alternative purposes, such as employment decisions.\textsuperscript{81}

\textsuperscript{72} Id.
\textsuperscript{73} Id.
\textsuperscript{74} \textit{See id.} at 14.
\textsuperscript{75} Id.
\textsuperscript{76} \textit{Id.; see} Evans, \textit{supra} note 59, at 250.
\textsuperscript{77} Brown, \textit{supra} note 16, at 15–16.
\textsuperscript{78} Id.
\textsuperscript{80} \textit{See Orion}, 208 F. Supp. 3d at 993.
\textsuperscript{81} \textit{See id.} at 992–93.
The next Section further explains the possibility of adverse employment actions resulting from fitness tracking and establishes why adverse employment actions are a greater concern than data security.

**B. Adverse Employment Actions**

A SimplyHired.com survey of jobseekers in the 2012 college graduating class showed that students’ top concern was job security.\(^82\) In fact, 33 percent of students said job security was their top concern, as opposed to salary (23 percent) and benefits (23 percent).\(^83\) This suggests that, while benefits such as optimal health insurance coverage at lower costs are important, young jobseekers often value job security more than they value health benefits. Taking a step further, this data suggests that most jobseekers would prefer not to wear a fitness tracking device and receive greater health benefits if it means that their job security would suffer.

Aside from new jobseekers, current employees are also concerned about job security.\(^84\) The 2011 Job Satisfaction and Engagement Research Report, released by the Society for Human Resource Management, showed that 63 percent of respondents valued job security as “very important” to them.\(^85\) However, only 28 percent of respondents were “very satisfied” with their job security.\(^86\) Considering that more than half of respondents valued job security highly, but less than one-third were pleased with their job security, it is unlikely that the responders would have worn fitness tracking devices if the devices could further jeopardize their job security—even in return for lower health costs.

While both of these statistics gauged job security shortly after the 2008 financial crisis, there is no evidence suggesting that job security concerns were only prevalent in those surveys because of recent economic struggles. If there were any statistical influence based on the aftermath of the financial crisis, it likely would not be significant enough to move job security from a top concern to a


\(^{83}\) Id.

\(^{84}\) SOCY FOR HUMAN RES. MGMT., supra note 19, at 4.

\(^{85}\) Id.

\(^{86}\) Id. at 53.
Further, issues implicating job security concerns frequently arise, such as those experienced by UK information technology (IT) professionals in light of Brexit (the United Kingdom’s departure from the European Union). A recent poll showed that 40 percent of UK IT professionals said Brexit made their job less secure, as opposed to just 13 percent saying that their positions became more secure. Thus, job security will almost certainly remain a concern in light of ever-changing circumstances in various workforces.

Employers’ use of health data also influences salary and opportunity for growth. Job security may be stable if an employer does not decide to hire or fire employees merely based on health data, but employers may use such data to make promotional decisions. For example, consider two employees that have no openly observable variables among them. Their age, experience, education, production, and attitude are all identical (an important, but surely not conclusive, list of attributes that may influence promotional decisions). However, consider that one employee has high cholesterol while the other does not. Their health, aside from cholesterol, is the same. It would make sense for the company to promote the employee that does not have high cholesterol, with the belief that the employee will encounter fewer potential health risks than the other employee in the future. The company may believe that the employee with lower cholesterol is able to work longer and more efficiently.

While the 2011 Job Satisfaction and Engagement Report showed that job security was a top concern, participants indicated benefits and salary were also important concerns. It would be difficult to find an employee who does not agree that the advantages of a promotion are desirable and important. Therefore, employee concerns over employers using health data for promotional decisions, not just hiring and firing decisions, are also prevalent and important.

87. See id. at 23, 40. Because job security is such a significant concern, the recession likely was not the reason for it being a concern in the first place.
89. Id.
90. Consider here that “high cholesterol” refers to high levels of low-density lipoprotein (LDL), or “bad” cholesterol, that makes up an unhealthy cholesterol level—not simply a higher total cholesterol that is healthier than a lower total cholesterol based on the combination of LDL and high-density lipoprotein (HDL) levels. See What Is Cholesterol?, NAT’L INST. HEALTH, https://www.nhlbi.nih.gov/health/health-topics/topics/hbc [https://perma.cc/ZKK9-E76M] (last visited Sept. 27, 2017).
91. SOCY FOR HUMAN RES. MGMT., supra note 19, at 4.
Not only are employment actions a concern for employees, but employees may not realize that data recorded through fitness trackers can indicate a flaw in their prospective productivity or growth in the workforce. For example, an employee may wear a fitness tracker with the idea that the employer will use his or her exercise habits for health insurance purposes. However, exercise habits can lead to inferences of impulsivity and inability to delay gratification, which correlate with alcohol and drug abuse, eating disorders, cigarette smoking, higher credit card debt, and lower credit scores. Further, access to sleeping data could be used to infer poor psychological well-being, poor cognitive performance, anger, depression, and other health problems. Providing access to seemingly harmless data for health insurance purposes could lead to inferences that adversely affect an employee’s job security or promotional prospects.

With the threat of employers relying on this health data for employment decisions, wearing fitness trackers for health insurance reasons suddenly becomes less appealing for employees. Further, some trackers are mandatory during employment, which may factor in to an employee’s decision to work for a company. Because employees value job security more than benefits and consider growth and salary important, health insurance advantages that come with fitness tracking may not be worth the risk of health data being used for employment decisions influencing job security, salary, and growth opportunities.

This Note suggests that adverse employment decisions based on health data are the problems most direly in need of a solution. While data privacy is surely a concern, what can be done with that data poses a more immediate threat to employees. Employees may be comfortable with their health data being collected and formed into aggregate statistics by third parties and then used by their employers solely for health insurance reasons. This scenario offers benefits for the employer that trickle down to the employees in lower premiums, lower copays, and wider insurance coverage. While Orion shows how employees may be comfortable with third parties collecting and managing this data for the employer to later receive aggregate,

---

93. Id.
94. Id.
95. See Brown, supra note 16, at 14.
anonymous data, it also demonstrates how there can still be a concern that the employer will receive the data despite the third parties’ privacy policies.\textsuperscript{98} For this reason, employees are concerned not only with keeping the information secure but also with keeping data away from the party that can use it adversely against them.\textsuperscript{99} The true employee concern is not simply the threat of the data being revealed, but the threat that the data can harm them in another manner. Therefore, while data privacy is a concern for employees,\textsuperscript{100} this Note emphasizes the need to safeguard employees from employment decisions being made based on their health data. This would eliminate the concerns that fitness tracking can influence jobs, and leave solely the concern that data may be shared or accessed through security breaches. Until there is an adequate system for protecting information collected from tracking devices, the law needs to protect employees from the manners in which employers can use such data against them. Part III discusses current options for data security and why the current options are insufficient to protect employees and their data.

III. CURRENT SOLUTIONS FOR PROTECTING DATA AND THEIR INADEQUACY

To solve the problem of employers using health data from wearables to make employment decisions, federal law must protect either (1) the data collected from tracking devices or (2) employees from employers using such data for employment decisions. This Part explores how current avenues for protecting data are inadequate, showing that protecting employees from adverse employment decisions should be the priority until privacy and data security laws can provide real protection. This Part also addresses inadequate protection under HIPAA and the Computer Fraud and Abuse Act (CFAA) before presenting an extensive analysis of the ADA and its recent case law developments. While the ADA proves inadequate to protect the health data, a deeper dive into relevant case law shows that additional EEOC regulation can protect employees.


\textsuperscript{99} See id.

\textsuperscript{100} Brown, supra note 16, at 10.
A. Health Insurance Portability and Accountability Act

Most people know HIPAA as the federal law that protects confidentiality of patients’ health information.101 HIPAA prohibits unauthorized disclosure of protected health information except for legitimate medical, business, or public health use.102 HIPAA only applies to “covered entities,” including health plans, healthcare “clearinghouses” that change health information from one format to another, and healthcare providers.103 These covered entities and their business associates are the only entities that HIPAA restricts from disclosing health information.104

The health information that HIPAA protects includes any information created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse, and relates to health, conditions, healthcare provisions, or healthcare payments of an individual.105 Health information includes “individually identifiable health information,” which is health information that identifies an individual or that can be used to identify an individual.106 Initially, it appears as though the information tracked through fitness devices would be covered by HIPAA because healthcare providers and business associates cannot disclose the information to employers. However, data from tracking devices are technically disclosed by the company that manufactures the device through the company’s app or website that tracks the data.107 HIPAA does not cover this data because the data passes from the individual to a third party (the device manufacturer) and the third party distributes the data thereafter.108

---


103. 45 C.F.R. § 160.103 (2017).

104. See id. § 160.102.

105. Id. § 160.103.

106. Id.


Finally, HIPAA does not provide a private right of action to plaintiffs who suffer a violation of their privacy rights under HIPAA. This ultimately leaves employees with no avenue for enforcing their privacy rights, even if HIPAA covers reidentified information or the information relayed from third parties to covered entities. Therefore, HIPAA does not provide sufficient protection and subjects employees to the possibility of employers accessing their data, even if third-party vendors who manage the data are subject to HIPAA restrictions.

Elizabeth Brown suggests extending HIPAA’s “covered entities” language to employers, thereby protecting employees from misuse of their health data. While extended HIPAA coverage would resolve the issue, Brown also suggests that Congress needs to ultimately amend HIPAA to solve other similar issues. These changes present a viable solution, but there has been no recent congressional momentum to include employers under HIPAA’s covered entities. Before extending privacy and data security coverage through amendments and extended coverage, the law should protect employees from adverse employment actions by using solutions that are easier to implement, as suggested below.

B. Computer Fraud and Abuse Act

The CFAA criminalizes intentionally accessing a “computer” without authorization, in a variety of enumerated manners. Unlike HIPAA, the CFAA provides a private right of action under 18 U.S.C. § 1030(g). Under a private civil claim, a plaintiff must prove: (1) damage or loss (2) caused by (3) a violation of one of the substantive

110. See also Amelia R. Montgomery, Note, Just What the Doctor Ordered: Protecting Privacy Without Impeding Development of Digital Pills, 19 VAND. J. ENT. & TECH. L. 147, 166 (2016) (“[T]he ease of re-identification of anonymized datasets should impress upon regulators and lawmakers that laws and regulations that seek to protect privacy by requiring anonymization, such as HIPAA’s Privacy Rule, are inadequate[.]”).
112. Id. at 47.
113. See infra Part IV.
provisions set forth in § 1030(a), and (4) conduct involving one of the factors in § 1030(c)(4)(A)(i)(I)–(V). Courts have not determined whether a “computer” entails tracking devices, but it is possible that courts may determine that a tracking device is a “computer” for purposes of the CFAA in the future. The US Court of Appeals for the Eighth Circuit determined that a cell phone is a “computer” under the CFAA, and interpreted the meaning of “computer” as “exceedingly broad.” Therefore, it is possible that the CFAA could soon cover tracking devices.

However, even if the CFAA covers tracking devices or other wearables, it would be difficult for an employee to bring a private action for an employer accessing data from the tracking device. Because an employer-provided tracking device requires some consent from the employee to be tracked, it is likely that courts would find that employees consented to the tracking and, therefore, that employers are not in violation of the CFAA by accessing the information. There is no string of established case law on the application of the CFAA to tracking devices, so employees cannot rely on protection from the CFAA either.

C. Americans with Disabilities Act

Under the ADA, a “covered entity” cannot require a medical examination or make inquiries as to whether an employee has a disability and the severity of the disability, unless the examination or inquiry is job related and consistent with business necessity. However, the ADA contains a safe harbor that exempts some insurance plans from the prohibition on examinations and inquiries.

The safe harbor provides that the ADA does not prohibit a covered entity from “establishing, sponsoring, observing or administering the terms of a bona fide benefit plan that [is] based on underwriting risks, classifying risks, or administering such risks that are based on or not inconsistent with State law.”

116. Section 1030(a) sets forth seven actionable activities. See id. § 1030(a)(1)–(7).
117. See id. § 1030(g). Sub-clauses (I)–(V) of § 1030(c)(4)(A)(i) set forth particular circumstances, such as physical injury to a person or a threat to public health. Id. § 1030(c)(4)(A)(i)(I)–(V).
122. Id.
In Seff v. Broward County, the Eleventh Circuit found that it was lawful to deduct $20 from employees’ biweekly paychecks if the employees refused to participate in an employee wellness program but still wanted to participate in the group health insurance plan. There, Florida’s Broward County offered group health insurance to its employees. In 2009, employees enrolled in the group plan became eligible to participate in a new employee wellness program sponsored by the county’s health insurance provider. The employee wellness program required employees to complete a biometric screening and a HRA. The healthcare provider would then use the data collected from the employee wellness program to identify employees that had asthma, hypertension, diabetes, congestive heart failure, or kidney disease, and subsequently offer those employees the opportunity to participate in a disease management program.

Employees could enroll in the Broward County group health plan without participating in the employee wellness program. However, beginning in April 2010, Broward County imposed a $20 charge on biweekly paychecks of employees enrolled in the group health plan but not participating in the employee wellness program. Broward County eventually stopped the charges in January 2011, but former employee Seff filed a class action on behalf of employees who incurred the $20 charges. Seff claimed that the employee wellness program’s testing requirements violated the ADA’s prohibition against medical examinations and disability-related inquiries.

The district court found that the employee wellness program was a “term” of a bona fide benefit plan—the Broward County group health plan—under the ADA safe harbor provision. Affirming the district court, the Eleventh Circuit found the employee wellness program was part of the contract that provided Broward County with a group health plan. The Eleventh Circuit pointed to the fact that Broward County advertised the program as part of its group health

---

123. Seff v. Broward Cnty., 691 F.3d 1221 (11th Cir. 2012).
124. Id. at 1222.
125. Id.
126. Id.
127. Id.
128. Id.
129. Id.
130. Id.
131. Id.
132. Id.
133. Id. at 1223.
134. Id. at 1224.
plan in employee handouts and that the program was only available to group health plan enrollees. The Seff decision sets precedent that employers can find methods for requiring health information from employees through group health plan terms. Indeed, the Eleventh Circuit even stated that a “term” of a bona fide health plan sufficient to meet the safe harbor provision of the ADA does not need to be expressly identified as a “term.” Because employees often want to take advantage of the favorable insurance plans that group health plans offer, this poses a problem for employees who do not want their health information circulated to their employers. If health insurance companies and employers make wearable device assessments a “term” of a group health plan, ADA protection will be inadequate for employees because of the safe harbor provision.

The EEOC also stepped in to protect employees from adverse actions that stem from employee health data. For example, in EEOC v. Flambeau, Inc., the EEOC sued defendant Flambeau, Inc., alleging that the company violated the ADA by conditioning participation in its health insurance plan on completion of a HRA and biometric screening test. The district court found that the assessment and test requirements were terms of the plan, similar to the term in the Seff case.

While the Flambeau case was consistent with the Eleventh Circuit’s Seff decision, the Orion decision held that there is room for the EEOC to regulate health data. In Orion, Chief Judge William C. Griesbach found that the EEOC has Chevron deference to create regulations about the ADA safe harbor provision, and he shed light on the purpose of the safe harbor provision.

---

135. Id.
136. See id.
137. Id.
139. Id. at 851.
140. Id. at 853–57; see Seff, 691 F.3d at 1224.
141. See Seff, 691 F.3d at 1224; see also Flambeau, 131 F. Supp. 3d at 851.
144. See Orion, 208 F. Supp. 3d at 995–99.
In Orion, a company implemented a self-insured health plan in belief that it would be more cost-effective and would improve the health of its employees. One year after implementing the self-insured plan, the company adopted an employee wellness program that contained three components—employees enrolled in the wellness program would have to (1) certify that they did not smoke, or otherwise pay an $80 surcharge per month; (2) exercise sixteen times per month on a range of motion machine in the company’s fitness center, or otherwise pay a $50 surcharge per month; and (3) complete a HRA at the beginning of the insurance year, or otherwise pay the entire monthly premium amount. The disputed component was the HRA, which included a health history questionnaire and biometric screening of blood pressure, height, weight, body circumference, and a blood analysis.

A vendor collected the information compiled from the HRA, which was sent to another vendor and then compiled and aggregated by another vendor before the company finally obtained the information in anonymous format. The company said that the purpose of receiving the aggregated data was to identify common health issues and improve the overall well-being of the employee base. By improving the health of the workforce, the company would also reduce its healthcare spending through its self-insured plan. While the company maintained that the health data would remain aggregated and the only entities with access were the vendors, employees were still concerned about the confidentiality of the information.

The EEOC brought the claim after employee Wendy Schobert elected not to participate in the HRA due to confidentiality concerns and was later fired under what the EEOC alleged was an anti-retaliation violation. For purposes of this Note, the anti-retaliation claim is irrelevant; however, the court’s analysis of the ADA safe harbor provision is vital. The EEOC alleged that the company violated the ADA by requiring employees enrolled in the

145.  Id. at 992.
146.  Id.
147.  Id.
148.  Id. at 992–93.
149.  Id. at 993.
150.  Id. at 992–93.
151.  The vendors considered the employees’ medical information to be protected by HIPAA.  Id. at 993.
152.  See id.
153.  Id. at 991.
154.  See id. at 995–99.
company’s self-insured health plan to either complete the HRA or pay 100 percent of the monthly premium.\textsuperscript{155} The company alleged that the ADA safe harbor should apply and presented an alternative theory that the medical examinations were lawful because they were part of a voluntary wellness program under 42 U.S.C. § 12112(d)(4)(B).\textsuperscript{156}

Chief Judge Greisbach considered the safe harbor and voluntary examination provisions in turn.\textsuperscript{157} The company relied on the \textit{Seff} and \textit{Flambeau} decisions,\textsuperscript{158} while the EEOC argued that those decisions were wrongly decided in light of a new EEOC regulation.\textsuperscript{159} The new EEOC regulation stated that the safe harbor provisions “do not apply to wellness programs, even if such plans are part of a covered entity’s health plan.”\textsuperscript{160} Chief Judge Greisbach first determined if the EEOC regulation received \textit{Chevron} deference in order to decide whether the regulation should bear substantial weight in the case.\textsuperscript{161} Courts apply \textit{Chevron} deference to an agency’s regulation “when it appears that Congress delegated authority to the agency generally to make rules carrying the force of law, and that the agency interpretation claiming deference was promulgated in the exercise of that authority.”\textsuperscript{162}

In determining whether the EEOC had regulatory authority, Chief Judge Griesbach found that Congress’s intent to limit or expand the EEOC’s regulatory authority was ambiguous.\textsuperscript{163} Chief Judge Griesbach noted that the ADA does not foreclose the EEOC from interpreting its provisions and, further, that Congress authorized the EEOC to create regulations to ensure that covered entities do not discriminate against individuals by conducting medical examinations and inquiries that are not job related or consistent with business necessity.\textsuperscript{164} \textit{Chevron} deference applies when a statute is ambiguous concerning the scope of authority and the agency’s interpretation of its
authority is reasonable and consistent with the statute.\textsuperscript{165} Chief Judge Griesbach found that the EEOC interpreted its authority under an ambiguous statute (the ADA) in a reasonable and consistent manner,\textsuperscript{166} therefore, the EEOC’s regulation clarifying the applicability of the ADA safe harbor provision was within the scope of the agency’s authority.\textsuperscript{167}

The company alleged that, even if the EEOC had authority to create regulations clarifying the safe harbor provision, the specific EEOC regulation was not entitled to \textit{Chevron} deference because it was contrary to the statute.\textsuperscript{168} Chief Judge Griesbach once again found that Congress spoke ambiguously on whether the safe harbor provision applied to involuntary medical examinations of a wellness program.\textsuperscript{169} Therefore, the EEOC’s regulation would be upheld if it was reasonable.\textsuperscript{170} Finding that the EEOC properly determined that Congress did not intend for the safe harbor to apply in this instance, Chief Judge Griesbach determined that the EEOC regulation was permissible.\textsuperscript{171}

Chief Judge Griesbach also dismissed an argument that \textit{Seff} barred the regulation, pointing out that the issue in \textit{Seff} was whether the wellness program was a “term” of a plan—not whether the safe harbor provision should apply to wellness programs altogether.\textsuperscript{172} He declined to adopt the \textit{Seff} and \textit{Flambeau} holdings,\textsuperscript{173} reasoning that the safe harbor provision is “a limited exception that was created ‘to protect the basic business operations of insurance companies.’”\textsuperscript{174} Chief Judge Griesbach noted that the company’s wellness program was only broadly, at best, related to insurance.\textsuperscript{175} Therefore, the safe harbor provision would not apply to the company’s wellness program regardless of the new EEOC regulation.\textsuperscript{176}

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{165} City of Arlington v. FCC, 569 U.S. 290, 296–97 (2013).
\item \textsuperscript{166} \textit{Orion}, 208 F. Supp. 3d at 996.
\item \textsuperscript{167} \textit{Id}.
\item \textsuperscript{168} \textit{Id}.
\item \textsuperscript{169} \textit{Id} at 997.
\item \textsuperscript{170} \textit{Id}.
\item \textsuperscript{171} \textit{Id}.
\item \textsuperscript{172} \textit{Id} at 998–99.
\item \textsuperscript{173} \textit{See Seff v. Broward Cty.}, 691 F.3d 1221, 1222 (11th Cir. 2012); Equal Emp’t Opportunity Comm’n v. Flambeau, Inc., 131 F. Supp. 3d 849, 851 (W.D. Wis. 2015).
\item \textsuperscript{174} \textit{Orion}, 208 F. Supp. 3d at 999 (quoting E. Pierce Blue, \textit{Wellness Programs, the ADA, and GINA}, 31 \textsc{Hofstra L. & Emp. L.J.} 367, 378 (2014)).
\item \textsuperscript{175} \textit{Id} at 999–1000.
\item \textsuperscript{176} \textit{Id} at 1000.
\end{enumerate}
\end{footnotesize}
However, Chief Judge Griesbach then considered whether the wellness program was “voluntary,” and thus not in violation of the ADA.\textsuperscript{177} The EEOC states that medical examinations are “voluntary” when the employer does not: (1) “require employees to participate,” (2) deny coverage under any group health plan to employees for nonparticipation, or (3) take any adverse action, retaliate against, or coerce employees who choose not to participate.\textsuperscript{178} Chief Judge Griesbach found, despite the fact that the company was making employees pay 100 percent of the monthly premium if they did not partake in the HRA, that the program was voluntary and optional.\textsuperscript{179} He noted that there are aspects to balance when considering whether to participate in a particular wellness program or not, and that the employee must make a choice regarding the costs and benefits of participation or nonparticipation.\textsuperscript{180}

Therefore, even though the safe harbor provision did not apply to the wellness program because of the new EEOC regulation and Chief Judge Griesbach’s refusal to follow the \textit{Seff} and \textit{Flambeau} holdings, the wellness program did not violate 42 U.S.C. § 12112(d)(4)(A)’s prohibition on medical examinations because the wellness program was voluntary.\textsuperscript{181}

While the \textit{Orion} holding found that the HRAs were lawful under the ADA because they were part of a voluntary wellness program,\textsuperscript{182} Chief Judge Griesbach also found that the EEOC has \textit{Chevron} deference to interpret and create regulations with regard to the ADA safe harbor provision.\textsuperscript{183} With \textit{Chevron} deference to interpret the ADA safe harbor provision, it is possible that the EEOC’s other regulations would bear considerable weight in cases and that the EEOC could create additional regulations on the issue.

Further, Chief Judge Griesbach’s analysis on the safe harbor provision, while dismissing the holdings in \textit{Seff} and \textit{Flambeau},\textsuperscript{184} sheds light on the purpose of the safe harbor provision.\textsuperscript{185} Chief Judge Griesbach stated that the safe harbor provision is meant to protect

\begin{itemize}
\item \textsuperscript{177} \textit{Id.} at 1000–01.
\item \textsuperscript{178} 29 C.F.R. § 1630.14(d)(2)(i)–(iii) (2017).
\item \textsuperscript{179} \textit{Orion}, 208 F. Supp. 3d at 1001.
\item \textsuperscript{180} \textit{Id.}
\item \textsuperscript{181} \textit{Id.} Voluntary examinations are acceptable examinations and inquiries. 42 U.S.C. § 12112(d)(4)(B) (2012).
\item \textsuperscript{182} \textit{Orion}, 208 F. Supp. 3d at 1001.
\item \textsuperscript{183} \textit{Id.} at 996.
\item \textsuperscript{184} \textit{See Seff} v. Broward Cty., 691 F.3d 1221, 1222 (11th Cir. 2012); Equal Emp’t Opportunity Comm’n v. Flambeau, Inc., 131 F. Supp. 3d 849, 851 (W.D. Wis. 2015).
\item \textsuperscript{185} \textit{See Orion}, 208 F. Supp. 3d at 999.
\end{itemize}
wellness programs related to insurance and is only available to those who “establish, sponsor, observe, or administer benefit plans.”\textsuperscript{186}

Overall, it is likely that courts would find that corporate wellness programs incorporating fitness tracking technology are “voluntary,” and thus that the examinations and inquiries performed by the tracking devices are permissible under the ADA.\textsuperscript{187} Even if courts did not recognize these fitness assessments and inquiries as permissible, corporations could likely restructure wellness programs so that the fitness tracking qualifies for the 42 U.S.C. § 12112(d)(4)(B) voluntary exception.\textsuperscript{188}

Therefore, under current laws and regulations, participation in a wellness program that includes fitness tracking through wearable technology will lead to lawful access to health data. There are no readily available avenues for protecting the health data itself.

IV. PROPOSED SOLUTIONS

To protect employees from employers adversely using health data collected through fitness trackers, this Note suggests two solutions stemming from Chief Judge Griesbach’s analysis giving deference to the EEOC’s interpretive authority.\textsuperscript{189} To recap, these solutions are necessary because health data collected through fitness tracking will be acquired through a voluntary examination or an examination protected by ADA safe harbors.\textsuperscript{190} As suggested earlier, protecting employees should actually be the primary concern because employees are chiefly concerned with job security and growth opportunities.\textsuperscript{191}

The two solutions suggest that courts should give deference to these regulations by relying on Chief Judge Griesbach’s \textit{Orion} analysis and the EEOC should amend current regulations to further protect employees.\textsuperscript{192} This Part also addresses efforts to eliminate \textit{Chevron} deference and urges courts to interpret the ADA to protect

\textsuperscript{186} \textit{Id.} at 1000 (quoting 29 C.F.R. § 1630.16(f)(3) (2016)).

\textsuperscript{187} \textit{See} 42 U.S.C. § 12112(d)(4)(B) (2012); \textit{see also Orion}, 208 F. Supp. 3d at 1001 (finding that a medical examination, because it was voluntary, was legal).

\textsuperscript{188} \textit{See} 42 U.S.C. § 12112(d)(4)(B). Considering Chief Judge Griesbach’s holding in \textit{Orion} that the wellness initiative was voluntary, it would not be difficult for corporations to structure their wellness initiatives so as to be considered voluntary. \textit{See Orion}, 208 F. Supp. 3d at 1001.

\textsuperscript{189} \textit{See Orion}, 208 F. Supp. 3d at 995–99.

\textsuperscript{190} \textit{See supra} Parts III.A & III.B (noting that HIPAA and CFAA protection is also inadequate).

\textsuperscript{191} \textit{See supra} notes 18–20, 82–91, 94, 96–97 and accompanying text.

\textsuperscript{192} \textit{See Orion}, 208 F. Supp. 3d at 995–99.
employees in a manner parallel with the suggested regulations—even if *Chevron* deference to the EEOC no longer applies.

A. Follow Chief Judge Griesbach by Giving Deference

In order for the proposed solutions to be effective, courts should give *Chevron* deference to the EEOC’s interpretations of the ADA. Chief Judge Griesbach found that the EEOC had rulemaking authority with regard to the ADA safe harbor provision,\textsuperscript{193} so there is an argument to be made that his decision only extended the EEOC’s authority to the safe harbor provision, rather than other provisions of the ADA. However, Chief Judge Griesbach analyzed the EEOC’s authority in a broad sense, stating that the ADA does not “limit the EEOC’s authority to creating regulations that solely interpret Title I.”\textsuperscript{194} Because Title I includes 42 U.S.C. § 12112(d) on medical examinations, the following suggested regulations interpreting that provision would receive *Chevron* deference if they are based on a permissible or reasonable construction of the statute.\textsuperscript{195}

Considering that Chief Judge Griesbach found the EEOC’s prohibition of the safe harbor provision’s applicability to wellness programs as reasonable,\textsuperscript{196} courts would likely find the following regulations to be reasonable constructions of the statute as well.\textsuperscript{197} This would be dependent on judges’ interpretations of the regulations and the ADA, but courts should follow Chief Judge Griesbach’s *Orion* analysis and afford *Chevron* deference to the suggested EEOC regulations, as well as current EEOC regulations interpreting the ADA.\textsuperscript{198}

B. Suggested Changes to Current Regulations

The following suggestions to change current ADA regulations would ensure confidentiality of employee health data and close the voluntary examination loophole. Courts should afford deference to these changes, and the regulations already in place, to protect employees in a manner consistent with the purpose of the ADA.

\begin{itemize}
\item \textsuperscript{193} *Id.* at 996.
\item \textsuperscript{194} *Id.; see also* 42 U.S.C. §§ 12101–17 (2012).
\item \textsuperscript{195} *See Orion*, 208 F. Supp. 3d at 996.
\item \textsuperscript{196} *See id.* at 997.
\item \textsuperscript{197} The suggested regulations are not nearly as overpowering as the EEOC regulation stating that the safe harbor provisions do not apply to certain kinds of programs. *See* 29 C.F.R. § 1630.1(d)(6) (2017).
\item \textsuperscript{198} *See Orion*, 208 F. Supp. 3d at 995–99.
\end{itemize}
1. Bolster Confidentiality

The first proposed change is an effort to ensure employees that other employees, specifically management-level employees, cannot access health data. While most plans allege that the data will only be used for insurance purposes and that adverse employment actions based on the data cannot be taken against employees, there is no guarantee that employers will not, at least implicitly (if not explicitly), base employment decisions on health data. Wendy Schobert’s concerns in Orion, despite the company’s confidentiality promises, show that employees remain skeptical over the confidentiality of their health data.199 Along with real instances of employees being fired for health reasons—such as Lisa Harrison’s weight,200 Edward Bess’s blood pressure,201 or Scott Rodrigues’s smoking habits202—employees face a threat that employers will increasingly make employment decisions based on this newly accessible data.

Current EEOC regulations state that a covered entity’s examinations are confidential, except that “supervisors and managers may be informed regarding necessary restrictions on the work or duties of the employee and necessary accommodations.”203 The regulation also permits first aid and safety personnel to be informed of the information when the information suggests a possible need for emergency treatment.204

To ensure that management does not gain access to the information, the EEOC should withdraw the exception that allows supervisors and managers to be informed of health data. While the exception appears narrow, one can imagine a scenario in which an employer requests data from a covered entity for what the employer describes is information on “necessary restrictions” on work or duties. The employer could then implicitly or explicitly use the data to make a future promotional decision. To safeguard employees from any possibility of management using this exception to access health information, the EEOC should eliminate the exception altogether. This would eliminate any possibility of management using the

199. See id. at 993.
204. Id. § 1630.14(c)(1)(ii). Section 1630.14(c)(1)(iii) also provides that government officials can gain access to the information when needed to investigate compliance with the ADA. Id. § 1630.14(c)(1)(iii).
information against employees and increase employee confidence in the confidentiality of the health insurance programs. Therefore, employers would have a stronger participation rate in the fitness tracking programs and an increased chance at receiving health insurance subsidies.

Eliminating the exception would leave a complication: nobody would have access to health data that is truly for the use of necessary restrictions on duties and workplace accommodations. Therefore, this Note suggests an addition to the safety personnel exception,²⁰⁵ to state that safety personnel can have access to health data when needed to determine workplace restrictions or accommodations. The EEOC should then define “safety personnel” to include a designated employee, whether a specific safety personnel manager or specialized human resources employee, that is the only employee with access to the information for risk and safety reasons. Then, an employee with specifically described safety authority will have access to the information and be able to address safety concerns. The definition of “safety personnel” would require this employee to be separate from typical management-level employees, to ensure severability from regular business decisions.²⁰⁶

The new regulation would not allow anyone to access employee health data tracked through wearable devices, except for an employee designated as part of “safety personnel.” This ensures employees that management will not be able to legally access their health data in an identifiable format and safeguards employees from management using health data, explicitly or implicitly, when making employment decisions.

²⁰⁵.  *Id.* § 1630.14(c)(1)(ii).
²⁰⁶.  See *id.* There would likely be employer pushback against this EEOC regulation because of the need for either an additional safety personnel employee or an increase in an existing employee’s duties. Allowing a human resources manager, who is separate from the rest of management, to qualify as a designated safety personnel employee would be more efficient for corporations from a fiscal standpoint. The cost of allocating additional responsibility to one employee would not be a large enough burden to compromise confidentiality and employee trust in the confidentiality procedures.
2. Eliminate the Voluntary Examination Loophole

While the first proposed regulation change would reinforce confidentiality, the voluntary examination exception still subjects employees to management accessing health data. The following proposed changes assure that employers cannot use data obtained through a voluntary examination for any reason other than insurance-related purposes.

The current regulation on voluntary examinations states that an examination is voluntary if it “[d]oes not require employees to participate,” does not deny or limit coverage to employees who do not participate in the voluntary examinations, and “[d]oes not take any adverse employment action or retaliate against, interfere with, coerce, intimidate, or threaten employees.” The EEOC should extend the third requirement to state that employers cannot take any adverse employment action not only in the course of collecting the data and enrolling in the voluntary program, but also after employees have agreed to participate in the program. As the regulation currently stands, it may only protect adverse employment actions taken against employees who oppose the voluntary examination in the first place. Clarifying and extending the protection to include any action during and after the course of data collection would ensure that employees participating in the program are also protected.

Finally, the EEOC should create an additional regulation which states that any examination that provides for the use of data for reasons other than insurance-related purposes will automatically be considered involuntary. This effectively eliminates the possibility of employees assenting to their examinations being used for noninsurance purposes. The additional regulation would be implemented to ensure that employers cannot use their bargaining power to require employees to assent to their data being used for noninsurance purposes. Furthermore, this change would only allow employers to take advantage of the 42 U.S.C. § 12112(d)(4)(B)

207. See 42 U.S.C. § 12112(d)(4)(B) (2012); Equal Emp’t Opportunity Comm’n v. Orion Energy Sys., Inc., 208 F. Supp. 3d 989, 1000–01 (E.D. Wis. 2016) (finding that, even though the safe harbor provision did not apply, the medical examination was voluntary and thus a legal examination).

208. 29 C.F.R. § 1630.14(d)(2)(i)–(iii).

209. In contrast, the provision could currently be read as only safeguarding employees who dissent from the program. See id. § 1630.14(d)(2)(iii).

210. Surely, some employees would feel unsettled by the fact that they cannot voluntarily agree to the use of their medical information for noninsurance purposes. However, this additional regulation would merely eliminate the possibility of lawful ADA examinations being used for such purposes. Employees could voluntarily disclose their information through other methods, which simply would not receive ADA protection of any sort.
voluntary examination exception if they use the voluntary examinations for insurance-related purposes.\textsuperscript{211}

The regulation should also clarify that the language in the voluntary examination exception, stating that “covered entit[ies] may make inquiries into the ability of an employee to perform job-related functions,”\textsuperscript{212} means that employers can only inquire for safety and accommodation reasons consistent with the proposed confidentiality regulations set forth above, and only to the designated safety personnel.\textsuperscript{213} Altogether, the additional regulation would only allow inquiries for insurance purposes or safety reasons consistent with confidentiality requirements.

\textbf{C. Insignificance of Eliminating Chevron Deference}

The regulation additions and changes suggested above would ensure that health data is only accessible by “safety personnel” rather than management, and that the voluntary examination exception is only applicable to inquiries used for insurance purposes. Therefore, if management-level employees access the health data, or the health data is used for any reason other than insurance purposes, it will be an unlawful use of the data. These regulations would provide protection to employees if they are found reasonable by courts and thus receive \textit{Chevron} deference. As stated previously, these regulations would likely receive \textit{Chevron} deference because they are consistent with the purpose of the ADA—combatting disability-based discrimination.\textsuperscript{214}

However, it must be noted that there have been recent efforts to alter \textit{Chevron} deference and afford courts de novo review when interpreting statutory provisions and rules.\textsuperscript{215} These efforts may appear to thwart the suggested solutions, but courts should interpret the ADA consistently with its purpose, regardless of deference to EEOC regulations. Even interpreting the ADA de novo, courts should recognize the threats that confidentiality concerns and voluntary examinations can pose toward employees.

Without \textit{Chevron} deference, courts should still interpret the ADA in a manner consistent with the suggested regulations because

\begin{footnotesize}
\begin{enumerate}
\item[(211)] See 42 U.S.C. § 12112(d)(4)(B).
\item[(212)] Id.
\item[(213)] See supra Part IV.B.1.
\item[(214)] See § 12101(b)(1)–(4).
\end{enumerate}
\end{footnotesize}
they serve the purpose of the ADA. Interpreting the statute in a manner inconsistent with the proposed solutions would provide loopholes for employers to access health data and use it against employees, which would undermine the ADA. Therefore, *Chevron* deference provides a smooth path for protecting employees based on EEOC regulations, but courts would interpret the ADA in the same protective manner even if reviewing the statutes de novo. The future of *Chevron* deference is insignificant because courts, if interpreting the ADA in coherence with its purpose, should provide employees with the same safeguards as the EEOC regulations and proposed solutions.

V. CONCLUSION

Employers are increasingly tracking fitness and collecting health data for insurance advantages, but they may use this data for other purposes, such as promotional and hiring decisions. Employees, primarily concerned with job security and growth opportunities, would not want their employment threatened by management reaching a decision based on employee health rather than workplace production. Therefore, employees having their health data collected and tracked need protection from employers making employment decisions based on this data.

Current privacy and data security laws are inadequate for protecting the data and maintaining confidentiality because of the various avenues for access. New and revised EEOC regulations interpreting the ADA are necessary to protect employees. Chief Judge William C. Griesbach afforded deference to the EEOC’s interpretations of the ADA, and courts should follow his decision by affording deference to the EEOC’s future interpretations. If the EEOC changes current regulations to prohibit management-level access to the health data and states that voluntary examinations can only be used for insurance-related purposes, the ADA will provide adequate protection for employees. If courts review statutes de novo rather than with deference to agency interpretations, they should still interpret the ADA to protect employees from adverse employment actions and management-level access to their health data.

The proposed solutions provide temporary relief for employees whose data may be accessed and used for purposes inconsistent with health insurance advantages. While the solutions safeguard employees from adverse employment actions, data security and privacy laws will eventually need to protect the tracked data. For the

time being, protecting employees is a readily available option based on current case law and regulations. However, because of the emergent nature of technology, protecting the health data and ensuring that the data is only accessible for its intended purposes is the only solution that will provide ongoing protection. Until privacy and data security laws can provide ongoing data protection by virtue of newly enacted laws or amendments to existing laws, the suggested solutions can protect employees in the interim.

*J.T. Parisi*