WORLD PRIVACY FORUM

3108 Fifth Avenue
Suite B
San Diego, CA 92103

# Comments of World Privacy Forum

## To Equal Employment Opportunity Commission

## Regarding Title II of the Genetic Information Nondiscrimination Act of 2008, Revisions to the Wellness Program Exception

*via Federal eRulemaking portal* [*www.regulations.gov*](http://www.regulations.gov)

Bernadette Wilson
Acting Executive Officer, Executive Secretariat
U.S. Equal Employment Opportunity Commission
131 M Street NE., Washington, DC 20507

**Re: EEOC RIN number 3046-AB02**

January 20, 2016

The World Privacy Forum welcomes this opportunity to submit comments on the Equal Employment Opportunity Commission's proposed rule amending the regulations implementing Title II of the Genetic Information Nondiscrimination Act of 2008 as they relate to employer wellness programs. The proposal appears in the Federal Register at https://www.gpo.gov/fdsys/pkg/FR-2015-12-07/pdf/2015-30807.pdf , 80 Federal Register 75956 (Dec. 7, 2015). RIN number 3046–AB02.

The World Privacy Forum is a non-profit public interest research and consumer education group. We have published many research papers and policy comments focused on privacy and security issues. Much of our work explores technology and health-related privacy issues, biometrics, consent, data analytics, and many other rapidly evolving areas of privacy. You can see our publications and more information at www.worldprivacyforum.org.

## I . General Comments

In general, the World Privacy Forum (WPF) supports the Commission's goal of ensuring that wellness programs do not contribute to genetic discrimination in the workplace. We are not sure, however, that the proposed rule strikes the right balance among all the competing interests. We begin by offering some general observations about the issues involved in this rulemaking, and then we respond to specific parts of the NPRM

### A. PII and Wellness Programs

We are concerned about the privacy of personally identifiable information (PII) collected and used in wellness programs. Much wellness information falls outside of the protections of the privacy and security rules of the Health Insurance Portability and Accountability Act (HIPAA). Much wellness program information also falls outside of the protections of other federal and state privacy laws. Individuals often erroneously think that the HIPAA rules protect the privacy of any health information, and they may let their privacy guard down as a result. This is particularly true of wellness programs, and it is a serious concern that remains unaddressed at all levels.

When wellness programs employ health and fitness (or other types of ) monitoring devices manufactured and supported by a variety of independent companies, the companies or intermediaries may use the personal information generated in ways wholly unrelated to the wellness program. The consumer wellness information gathered in this scenario is typically not subject to any health privacy law. Each device manufacturer or other independent vendor supporting wellness programs can have its own privacy policy, and some have no privacy policy, or have a privacy policy that offers no meaningful protections to individuals. Further, company privacy policies are typically subject to change at the whim of a company, so if a policy actually offers real privacy protections, the protections can disappear at any time and often without notice.[1]

There are many examples of health and fitness monitoring devices, mechanisms, and processes that allow for information sharing at a variety of levels, from APIs to aggregate sharing to check-box consent for use of the data in human subject-related research to use for predictive analytics

---

[1] The problem of material retroactive changes in privacy policies has been analyzed at length by the FTC. *In The Matter of Gateway Corp.* was an important FTC case in this regard. See https://www.ftc.gov/enforcement/cases-proceedings/042-3047/gateway-learning-corp-matter. See also: https://www.ftc.gov/news-events/press-releases/2004/07/gateway-learning-settles-ftc-privacy-charges.The issue of material changes to privacy policies is also relevant in the area of mergers, which is relevant to the nascent fitness and health device market, which we expect to undergo much change in the next five to ten years. See FTC, Mergers and policy changes: https://www.ftc.gov/news-events/blogs/businessblog/2015/03/mergers-privacy-promises .

about individual consumers or groups of consumers.[2] Employers offering wellness plans that allow unfettered data sharing and secondary use of consumer data may not fully understand the extent to which identifiable or re-identifiable data about individual consumers may be entering the secondary marketplace. Employers may be incentivized or pressured to prioritize lowering employee data costs over taking care of consumer data privacy impacts.

Device manufacturers are not the only merchants in the wellness arena that may exploit personal information. Wellness program operators may do the same. We are not aware of any even-handed privacy best practices for wellness activities. In fact, the business proposition of wellness vendors often depends on collecting, combining and analyzing data from many sources, ranging from health claims to detailed geo-location data to records of grocery purchases. Employers may not be sufficiently motivated to control secondary uses of wellness information about their employees, and the employees have no leverage, even if they understand how a wellness program many use or misuse employee data. That being said, it would be unusual for most employees to have successfully navigated the labyrinthine law around wellness programs and HIPAA. It is not a surprise that few employees genuinely understand the risks to their personal data in some corporate wellness programs.

The result is that personally identifiable information that starts out as part of a wellness program may become input to American marketers, database companies, and other data profilers. Worse, the consequences of marketing uses of health information are likely to work at cross-purposes with the goals of wellness programs. When marketers identify individuals who are overweight, suffer from chronic diseases, or have unhealthy habits, the marketers will be armed with the information to selectively target and sell vulnerable individuals a variety of goods and services that are not necessarily in the best interest of those individuals.[3]

Regrettably, we now know that not all companies are good actors. Due to a profound lack of regulatory control in this area, we have learned through a variety of FTC enforcement actions, reports, and other research, including our own, that marketers can and do sell dubious remedies and in some cases, additional opportunities to engage in unhealthy habits. Even if wellness

---

[2] "The New World of Health Sensors" is a video WPF prepared for a 2015 presentation at the Georgia Technology Institute. It provides a helpful overview of fitness devices, biosensors, and device trends. The video reviews the newest devices released at the 2015 Consumer Electronics Show, and is available online: https://www.worldprivacyforum.org/2015/03/video-the-new-world-of-health-sensors/. Additionally, WPF has a broader health technology video series exploring other fitness and health technology devices that may be helpful: https://www.worldprivacyforum.org/category/video-health-tech-series/.

[3] WPF has written and testified extensively about data broker activities in regards to health data. See, for example, our Congressional testimony on data brokers: (2013) http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=e290bd4e-66e4-42ad-94c5fcd4f9987781. See also: (2011) http://www.worldprivacyforum.org/wpcontent/uploads/2011/10/PamDixonConsumerExpectationTestimonyfsshort.pdf. See also: (2009) http://www.worldprivacyforum.org/wp-content/uploads/2009/11/TestimonyofPamDixonfs.pdf.

programs first aggregate or de-identify personally identifiable information from wellness programs, the use of that information to target ads and services will have the same negative health effects as ads based on identifiable data.

For more on commercial uses of personal information, we direct you to the WPF report titled *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future*. The report, which has been cited by both the White House Big Data report and the FTC Big Data Report among others, documents how marketers, profilers, and advertisers collect personal data from an increasing number of available sources and use that data to make decisions about and present offers, goods, and services to individuals. The information may affect individual lives and opportunities in many meaningful ways, most of them totally opaque to the individuals. Marketers especially prize health data. Increasing revenues is the priority of marketers, not increasing the health of those who receive offers and advertising. The WPF report is available at https://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secretconsumer-scores-threaten-your-privacy-and-your-future/.

What we have just described is the background and context of wellness programs. You cannot automatically assume that wellness programs are neutral programs designed to help employees manage and improve their health. Whatever else they may or may not accomplish, wellness programs often collect and disseminate personal health information to an unknown and unknowable number of marketers, database companies, and other data profilers. The personal health information shared with these commercial companies has no privacy protection under HIPAA or other law. Wellness programs evade the restrictions on the use and disclosure of health information imposed on employers by law. Wellness program operators and others profit from the use of the information, and there can be no guarantee that the information will be used to benefit either employers or employees.

### B. Potential for conflicts within families

Wellness programs have the potential to create conflicts within families. If programs demand that family members covered by a worker's health insurance comply with testing, monitoring, or lifestyle requirements, the result is likely to be new tensions within a family. Individuals required to comply with demands from a spouse's wellness program may be unhappy about the obligations or about the sharing of information necessary to justify an exception. If requirements extend to children, teenagers may be unwilling to cooperate with their parents.

College students, especially those living away from home, may not comply with the demands made by the wellness program of a parent's employer. Other types of conflicts may arise when a marriage is under stress; spouses could be living under a separation agreement; or a family could be experiencing domestic violence.

Given the complexities of relationships within families, wellness programs could very well exacerbate existing tensions and thereby undermine rather than improve health. We believe that the only way to avoid family conflicts is to disallow entirely all incentives, whether positive or negative, for the participation in wellness programs of anyone other than the employee. This approach offers the only way to make wellness programs available without creating problems for families. We do not object if wellness programs are available to spouses and children, but there should be no incentives at all for their participation or non-participation.

### C. Fairness and due process

We wonder whether wellness programs can be efficiently administered in a way that assures fairness and due process to individuals. A certain percentage of individuals will be unable to meet wellness program requirements for valid reasons such as pregnancy, disability, allergy, temporary illness, family emergencies, or travel. When an individual is unable to meet program requirements for medical reasons, wellness programs must provide an alternative. Proving the excuse for non-involvement may be cumbersome, expensive, and disputatious.

We note that individuals with orphan and rare diseases -- and 30 million of these individuals exist -- may well have conditions which are diagnosed, but incurable. These individuals, particularly spouses of policy holders, may not wish to disclose these conditions to a plan or wellness program, particularly when viable treatments do not exist. Yet these same individuals may not be able to participate in the wellness program due to disabilities introduced by the illness. This puts individuals in a terrible position where having to prove medical reasons for non-involvement offers only downsides for them.

The requirement for a wellness program to provide an alternative does not apply to those who cannot participate for non-medical reasons. Individuals facing penalties (and it does not matter whether the consequences are positive or negative) must have rights to present the reasons they did not comply with program standards. In some cases, obtaining a doctor’s letter may require an office visit, adding to the cost of health care and possibly requiring time off from work. In other cases, explaining a reason for non-participation may require an individual to reveal additional personal information about the individual or another person, such as an elderly parent or a child.

Convincing wellness program staff (who may not be health care professionals) to accept valid excuses will be a burden for employees, raise health care costs, and produce unfair results some of the time. Where a company has an incentive (by raising health care costs paid by employees), employer will increase the burden on employees and the barriers to fairness.

### D. Factual evidence of wellness program efficacy

We have doubts that wellness programs are, in fact, cost-effective measures that actually improve the health of employees and their families or that meaningfully lower health care costs across the board. We simply note the controversy about the value of wellness programs, a matter that is beyond our area of expertise to address. However, given the efficacy dispute as well as the negative privacy, fairness, and other consequences of wellness programs, we suggest that **each** wellness program must clearly demonstrate significant value. Obviously, wellness programs are in place and authorized by law today, but we suggest that the policy, facts, and science supporting wellness programs need regular reexamination to retest the premises of the programs with current facts.

In comments on previous NPRMs in this area, we recommended that the EEOC reopen its inquiry into wellness programs in four years and collect new data to determine if the elements of wellness programs rely on valid clinical evidence demonstrating effectiveness. We renew that recommendation here. The EEOC should require that wellness programs place evidence on the public record so that others have an opportunity to review and question that evidence.

## II. Specific Comments

### A. Purchasing Genetic Information

1. § 1635.8(b)(2)(i)(A)

> *First, we propose to add a new subsection to 29 CFR 1635.8(b)(2), to be numbered 1635.8(b)(2)(i)(A). It would explain that employers may request, require, or purchase genetic information as part of health or genetic services only when those services, including any acquisition of genetic information that is part of those services, are reasonably designed to promote health or prevent disease. In order to meet this standard, the program must have a reasonable chance of improving the health of, or preventing disease in, participating individuals, and must not be overly burdensome, a subterfuge for violating Title II of GINA or other laws prohibiting employment discrimination, or highly suspect in the method chosen to promote health or prevent disease. Collecting information on a health questionnaire without providing follow-up information or advice would not be reasonably designed to promote health or prevent disease. Additionally, a program is not reasonably designed to promote health or prevent disease if it imposes, as a condition of obtaining a reward, an overly burdensome amount of time for participation, requires unreasonably intrusive procedures, or places significant costs related to medical examinations on employees. A program is also not reasonably designed if it exists merely to shift costs from the covered entity to targeted employees based on their health.*

We have several concerns here. First, the words "purchase genetic information" are particularly troublesome. Where exactly does the Commission envision that an employer will purchase genetic information? HIPAA-covered entities cannot sell genetic or other PHI to employers. Will employers then purchase genetic information from websites, data brokers, and other commercial data base companies? Will the ability to purchase genetic information create a commercial marketplace for the purchase and sale of genetic information? We think that authorizing employers to buy genetic information may do just that, and we reiterate our concerns.

Second, our concern about purchasing genetic information is exacerbated by the standard that the NPRM proposes for health or genetic services: the services must be *reasonably designed to promote health or prevent disease*. This is a standard with virtually no meaning. Under it, any employer can decide for itself that any service is *reasonably designed*. The remaining words do not help at all: *the program must have a reasonable chance of improving the health of, or preventing disease in, participating individuals, and must not be overly burdensome, a subterfuge for violating Title II of GINA or other laws prohibiting employment discrimination, or highly suspect in the method chosen to promote health or prevent disease.* Reasonableness is a fine standard in some circumstances, but not here.

Any employer could decide that it is "reasonable" to purchase genetic information about employees from a commercial vendor because it might help some. Would that be reasonable? As long as an employer decides on its own motion what is reasonable, the answer will always be yes, regardless of the existence of a nexus between the genetic information purchased and the health program. Given that the odds that the EEOC or other independent agency will never review that decision, any employer can easily take the risk and proceed. The result is likely to be that the existing and wholly unregulated market for personal health information will increase in size and scope, to the detriment of every individual.

We propose instead that any acquisition of genetic information as part of health or genetic services be allowed only with the express and voluntary written consent of the data subject (including spouses and adult children) and then only after full disclosure of the type of information sought and the source of the information. Consents should be valid for no more than three months, and they should not be obtained as part of any other consent obtained from the data subject. **Consent to enroll in a wellness program should not also serve as consent for acquisition of genetic information from a third party, and there should be separate forms for consent with no penalty at all if an employee refuses consent for acquisition of information.** Any information acquired from a third party (or any source, including the employee) should be limited to the minimum necessary for the purpose, and there should be written documentation available to employees (and to the Commission) that explains what specific information is being acquired and the objective evidence that the information can be successfully used for the purpose of the acquisition.

Here's an example of how an employer should have to establish a nexus between information and its wellness program. If the program wants to collect genetic data for obesity management, it must document (1) that there is a scientifically demonstrated link between obesity and the genetic information used by the program, <u>and</u> (2) that program recommendations use the genetic profile of each individual. It should not be sufficient for the program to provide or cite to general nutrition advice.

**The Commission should expressly prohibit workplace wellness programs from accessing genetic information from other sources, such as patient claims data, medical records data, and commercial, for-profit organizations.** If employers obtains genetic data from other sources, the result may be that employees will broadly refuse genetic testing and treatment for fear that the information will end up back in the hands of the employer, its wellness vendor, the vendors' business associates, marketers, profilers, and database vendors.

### B. Inducements for Participation by a Spouse or Child

2. § 1635.8(b)(2)(iii)

> *A covered entity may offer, as part of its health plan, an inducement to an employee whose spouse (1) is covered under the employee's health plan; (2) receives health or genetic services offered by the employer, including as part of a wellness program; and (3) provides information about his or her current or past health status as part of a HRA. No inducement may be offered, however, in return for the spouse providing his or her own genetic information, including results of his or her genetic tests.*

For the reason stated above (Potential for conflicts within families), **we oppose any inducements for participation by a spouse or child**. Inducements will exacerbate any conflicts that exist in families over health or other matters. The result may be to worsen the mental and physical health of all family members and increase health care costs for physical and emotional ailments. Family turmoil and breakups affect health, job performance, and the well-being of children. If the Commission should not make a choice that has the potential to save employers a nickel while costing society a dollar. By allowing spouses and children to decide on their own to participate in a wellness program without any positive or negative consequences for the employee, family conflicts will be minimized.

### C. Incentives and Voluntariness

3. § 1635.8(b)(2)(iv)

> *The EEOC proposes that the maximum share of the inducement attributable to the employee's participation in an employer wellness program (or multiple employer wellness programs that request such information) be equal to 30 percent of the cost of self-only coverage.*

We seriously question whether a an inducement that costs an employee thousands of dollars can be genuinely voluntary. We know that others commenting on this rulemaking will provide better information about the actual costs that an employee may have to bear, and we know that those costs can be especially unaffordable for low and moderate wage earners. A limit of 30 percent is reasonable only if allowable incentives for participation in wellness program are only positive ones. Commission rules should ban negative incentives that impose additional costs on non-participating employees. If all incentives are positive, then the problem of offering incentives to employees who cannot participate in wellness programs for medical (or religious) reasons is a smaller concern.

### D. Prohibition of the Sale of Genetic Information

4. § 1635.8(b)(2)(vi)

> *Proposed section 1635.8(b)(2)(vi) would prohibit a covered entity from conditioning participation in a wellness program or an inducement on an employee, or the employee's spouse or other covered dependent, agreeing to the sale of genetic information or waiving protections provided under section 1635.9.*

We support this proposal to prohibit covered entities from conditioning employee participation in a program based on the sale of genetic information. However, we think that the word *sale* needs further clarification.

It is often the case in the personal information business that information will be exchanged, shared, licensed, used in a joint activity, or transferred in some other way that does not constitute a *sale*. Sometimes the holder of information uses it on behalf of a third person (e.g., sends a mailing on the third person's behalf). **The rule should apply to *sales, exchanges, sharing, uses, other transfers or disclosures, etc.*** The *etc.* is important because the definition should be as open ended as possible. This same broad concept of data transfer should apply throughout the rulemaking. We have consistently seen many work-arounds to the term "sale" in the marketplace, and this is an opportunity to effect a correction of this issue.

## III. Responses to Commission Questions

### A. Question 1:

> *(1) Whether employers that offer inducements to encourage the spouses of employees to disclose information about current or past health must also offer similar inducements to persons who choose not to disclose such information, but who instead provide certification from a medical professional stating that the spouse is under the care of a physician and that any medical risks identified by that physician are under active treatment.*

We believe that employers must be required to accept certifications from a medical professional chosen by an insured regarding the insured ability to participate in a wellness program. We would also allow an individual to self-certify. In both cases, a certification would shift the burden of proof to the employer to accept the certification or otherwise prove at its own expense that the employee is able to participate in the program.

### B. Question 2:

> *(2) Should the proposed authorization requirement apply only to wellness programs that offer more than de minimis rewards or penalties to employees whose spouses provide information about current or past health status as part of a HRA? If so, how should the Commission define "de minimis"?*

We see no reason to address the de minimis definition. All authorization and privacy requirements should apply to all wellness programs, regardless of their financial incentives or circumstances. Employers have many ways to pressure employees to participate that have nothing to do with financial rewards or penalties.

### C. Question 3:

> *(3) Which best practices or procedural safeguards ensure that employer-sponsored wellness programs are designed to promote health or prevent disease and do not operate to shift costs to employees with spouses who have health impairments or stigmatized conditions?*

First, no wellness program should be allowed to operate unless there is sufficient evidence to show that the specific program in use actually improves employee health and reduces costs. That may be the most important best practice to ensure that a wellness program offers real benefits to employers and employees. There should not be a burgeoning cottage industry of wellness programs springing up that simply make money because they have a new gadget or technique. Effective programs that can prove their results scientifically should win. They may have a new gadget or technique, but no matter what, they can prove their program works.

Second, there should be an independent due process mechanism that allows an aggrieved employee to object to how a wellness program applies to him or her and to show that the program operates unfairly in individual cases. The cost of the due process mechanism should be borne by the employer.

### D. Question 4

> *(4) Given that, in contrast to the status quo when the ADA was enacted, most employers today store personnel information electronically, and in light of increasingly frequent breaches to electronically stored employment records, should the rule include more specific guidance to employers regarding how to implement the requirements of 29 CFR 1635.9(a) for electronically stored records? If so,*

> *what procedures are needed to achieve GINA's goal of ensuring the confidentiality of genetic information with respect to electronic records stored by employers?*

There are existing standards for the security of health information issued by the Department of Health and Human Services as one of the HIPAA regulation. These security standards reflect best industry practices and are adaptable to the circumstances of each covered entity to which they apply. The HIPAA security standards apply to a wide range of health care providers and their business associates, including large and small entities.

The EEOC should require employers (and their business associates) that electronically store health information about employees to comply with the HIPAA security standards. There is no reason for the EEOC to reinvent the wheel here. Similarly, the HIPAA rule for breach notification can be applied to employers (and their business associates) for the same reasons.

**E. Question 5**

> *(5) In addition to any suggestions offered in response to the previous question, are there best practices or procedural safeguards to ensure that information about spouses' current health status is protected from disclosure?*

We repeat here our suggestion that no incentives (positive or negative) be allowed to induce participation in a wellness program by a spouse or child. That will allow those with special confidentiality concerns to simply decline to participate at no cost and with no risk to health information that they deem sensitive.

Frankly, we are not sure we understand the assumption behind this question that there might be different privacy and security rules for the information about some participants in a wellness program. We think that everyone should be protected by the same strong set of Fair Information Practices for privacy and the same high-level security protections.

If the question asks about the possibility that a wellness program may result in the sharing of information among family members, we can respond that there are serious concerns here. Apart from information sharing about minor children with parents, the sharing of health information among family members (employees, spouse, adult children) cannot be assumed to be routine within a family.

An employee, spouse, and adult child may have health issues that their do not always share within a family. For example, reports suggest that non-paternity occurs in as much as ten percent of cases. That is not the only reason for intra-family secrecy, but it serves the purpose. A wellness program should not allow any non-consensual sharing of information among participants in the same family.

**F. Question 6**

> (*6*) *Given concerns about privacy of genetic information, should the regulation restrict the collection of any genetic information by a workplace wellness program to only the minimum necessary to directly support the specific wellness activities, interventions, and advice provided through the program – namely information collected through the program's HRA and biometric screening? Should programs be prohibited from accessing genetic information from other sources, such as patient claims data and medical records data?*

We find this question disconcerting in some ways. Of course all collections of personal information of any type should be limited to the minimum necessary to accomplish the clearly defined purpose of the collection. We would give this answer no matter what type of data was being collected, let along genetic data. No one should collect any personal data unless it there is clear and convincing evidence that the data is necessary for a wellness program. Even then, use of patient claims data and medical record data should be expressly prohibited without the **affirmative, voluntary, and recent consent of the data subject**.

There is sufficient doubt about the efficacy of wellness programs in general that where there is a strong countervailing concern (privacy) for not sharing data, the sharing should be prohibited. Data sharing presents significant risks to data subjects, and sharing should be allowed only when there are demonstrable countervailing justifications and widespread public recognition and acceptance of those justifications.

## IV. Conclusion

The WPF is grateful for the opportunity to submit these comments regarding the Commission's Proposal. We welcome the opportunity to discuss these comments with the Commission and work with the Commission further on these issues.

Respectfully submitted,

Pam Dixon

Pam Dixon
Executive Director
World Privacy Forum