



Your Health Data for Lower Premiums? The Risks of Behavior-Based Insurance

Authors: AG Studies Staff and Policy Fellows

Imagine your health insurance premium changing based on how many steps you took last week, how well you slept, or even what you ate – all tracked by your smartwatch or phone app. This is the world of behavior-based health insurance (BBI), a rapidly growing trend where insurers use data about your daily habits to set prices and offer rewards. Proponents say it encourages healthier lifestyles and can lower costs. However, this constant monitoring raises serious questions about privacy, fairness, and consumer protection that demand attention, particularly from State AGs who work to safeguard our rights.

What is Behavior-Based Health Insurance (BBI)?

Unlike traditional health insurance, which mainly looks at your health history when you sign up, BBI uses technology – like fitness trackers, smartwatches, and health apps – to continuously collect data about your lifestyle. This can include:

- Physical activity (steps, workouts)
- Sleep patterns
- Heart rate
- Location data (where you exercise or spend time)
- Sometimes even dietary habits or medication reminders

Insurers use this stream of personal data to build a detailed profile of your health behaviors, adjusting your premiums or offering discounts based on whether you meet certain goals. As traditional insurance costs continue to rise, BBI programs might seem like an attractive, more affordable option.

The Hidden Costs: Privacy, Fairness, and Security Risks

While the promise of lower premiums is appealing, BBI comes with significant potential downsides that aren't always obvious:

1. **Your Life Under a Microscope:** Constant monitoring can reveal incredibly sensitive details about your life far beyond your step count – think mental health struggles inferred from sleep patterns, potential pregnancies detected through body temperature changes, or substance use habits hinted at by location data. Is this level of surveillance necessary for

insurance?

2. **Your Data for Sale?** The health data collected for your insurance policy might not stay there. It could potentially be sold to data brokers, pharmaceutical companies, or other third parties, often without your clear understanding or explicit consent.
3. **Guessing Games with Your Health:** Algorithms analyzing your data can make inferences about health conditions you haven't disclosed or might not even know you have, creating "shadow" health profiles outside your control.
4. **An Unequal Playing Field:** BBI might inadvertently discriminate against certain groups. For example, someone living in an unsafe neighborhood might struggle to meet daily step goals, or algorithms might penalize dietary habits common in specific cultures. This could worsen existing health disparities based on race, income, or disability.
5. **Is Your Data Safe?** Collecting vast amounts of intimate health data creates a tempting target for hackers. A data breach could expose extremely personal information, leading to identity theft or other harms.
6. **Feeling Forced Into It?** As traditional plans become more expensive, you might feel pressured to accept a BBI plan and its data tracking, even if you have privacy concerns. It might feel less like a choice and more like a necessity.
7. **The HIPAA Loophole:** Many people assume the health privacy law HIPAA protects all their health information. However, HIPAA often doesn't cover data collected directly by many consumer apps and wearables, especially when shared with insurers outside of a direct doctor-patient relationship.

What Protections Exist (and Where They Fall Short)

Laws are trying to catch up. Some states have passed specific rules about consumer health data privacy, requiring clearer consent and giving people more control. Federal laws like the Affordable Care Act offer some protection against discrimination based on health status, and the FTC has rules about health data breaches.

However, significant gaps remain. Many BBI programs operate in a grey area, potentially sidestepping existing protections. The complex algorithms used are often black boxes, making it hard to know if they are fair. And the sheer volume and sensitivity of the data being collected present unprecedented challenges.

How State Attorneys General Can Protect You

State Attorneys General (AGs) play a vital role as consumer watchdogs. They can tackle the risks of BBI by:

- **Investigating Misleading Claims:** Ensuring insurers are transparent and honest about how they collect, use, and protect your behavioral data.
- **Fighting Discrimination:** Using state and federal laws to challenge BBI practices or algorithms that unfairly penalize certain groups.
- **Enforcing Privacy Laws:** Applying state consumer protection and specific health data privacy laws (where they exist) to BBI programs.
- **Educating the Public:** Raising awareness about the potential risks and limitations of BBI plans.
- **Advocating for Stronger Rules:** Pushing for updated regulations that specifically address the unique challenges posed by continuous health monitoring and algorithmic decision-making in insurance.

Navigating the Future of Health Insurance

Behavior-based health insurance offers potential benefits but carries undeniable risks to our privacy and fairness. As this model expands, it's crucial that consumers understand the trade-offs involved. Strong oversight, clear regulations, and proactive enforcement by State Attorneys General are essential to ensure that the drive for innovation in insurance doesn't come at the cost of our fundamental rights and well-being.

Sources and Additional Reading

1. *60% of Health Payers to Offer Behavior-Based Insurance (BBI) by 2035*, ScienceSoft Forecasts, Bus.¹ Wire (Jan. 31, 2025), <https://www.businesswire.com/news/home/20250131681174/en/60-of-Health-Payers-to-Offer-Behavior-Based-Insurance-BBI-by-2035-ScienceSoft-Forecasts>.
2. *Behavior-Based Insurance (BBI) in Life and Health Products*, ScienceSoft, <https://www.scnsoft.com/finance/behavior-based-insurance-in-life-and-health-products> (last visited Apr. 14, 2025).
3. Elizabeth Snell, *Trends in Wearable Technology for Healthcare*, HealthTech (Mar. 11, 2024), <https://healthtechmagazine.net/article/2024/03/trends-wearable-technology-for-healthcare-perfcon>.
4. *Big Data Could Set Insurance Premiums. Minorities Could Pay the Price.*, ACLU (Oct. 25, 2017), <https://www.aclu.org/news/racial-justice/big-data-could-set-insurance-premiums-minorities-could>.
5. I. Glenn Cohen, *Personalized Medicine's Ragged Edge: Social Inequality, Genetic Discrimination, and the Role of the Law*, 18 Yale J. Health Pol'y L. & Ethics 1 (2019).
6. Marshall Allen, *Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates*, ProPublica (July 17, 2018), <https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates>.²

7. Kashmir Hill, *How Target Knew a High School Girl Was Pregnant Before Her Parents*, Time (Feb. 17, 2012), <https://techland.time.com/2012/02/17/how-target-knew-a-high-school-girl-was-pregnant-before-her-parents/>.
8. Angelique Carson, *Wearables: Where do they fall within the regulatory landscape?*, IAPP (Nov. 18, 2015), <https://iapp.org/news/a/wearables-where-do-they-fall-within-the-regulatory-landscape>.
9. *California expands scope of Confidentiality of Medical Information Act*, DLA Piper (Nov. 1, 2022), <https://www.dlapiper.com/es-pr/insights/publications/2022/11/california-expands-scope-of-confidentiality-of-medical-information-act>.
10. *Nevada Legislature Passes Consumer Health Data Privacy Bill*, WilmerHale (June 14, 2023), <https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20230614-nevada-legislature-passes-consumer-health-data-privacy-bill>.
11. Wash. Rev. Code Ann. ch. 19.373 (West 2024).
12. *The Connecticut Data Privacy Act*, Conn. Off. of the Att'y Gen., <https://portal.ct.gov/ag/sections/privacy/the-connecticut-data-privacy-act> (last visited Apr. 14, 2025).
13. Am. Med. Ass'n, *Privacy is Good Business: A case for strengthening HIPAA* (June 2022), <https://www.ama-assn.org/media/14241/download>.
14. *Complying with the FTC's Health Breach Notification Rule*, Fed. Trade Comm'n, <https://www.ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0> (last visited Apr. 14, 2025).
15. Md. Health Care Comm'n, *Patient-Generated Health Data (PGHD): Information for Providers*, https://mhcc.maryland.gov/mhcc/pages/hit/hit/documents/HIT_PGHD_Provider_Flyer.pdf (last visited Apr. 14, 2025).