The Institutes®
Griffith Foundation

The Institutes®
Griffith Foundation

Wearables and their Insurance Implications

The Promise and Potential Pitfalls of Wearables

The Griffith Insurance Education Foundation, an affiliate of The Institutes, is a 501(c)(3) non-profit, non-partisan, and non-advocative educational organization dedicated to the teaching and study of insurance and risk management.

In keeping with the non-partisan, non-advocative mission of The Griffith Foundation, I will keep my comments and contributions to today's program unbiased and purely educational.

Promise and Potential Pitfalls of Wearables

- Lots of promise – just like any health information system (e.g., genetic information → Personalized Medicine).
- Lots of potential pitfalls – effectiveness issues, privacy issues, equity issues.
- Characteristics of program adopted to use the information key!
- Regulatory measures that may help to enhance positives and limit negatives are also key!
- Much uncertainty likely to persist – as in any new application of information.

First person (user) direct advantages

- Provides information (and incentives) to improve healthy choices through monitoring.
- May allow people to obtain discounts on insurance and/or rewards from employers.
- Just plain interesting for some people to see results of monitoring. (e.g., city wide bike share with apps to record usage).

BUT!

- Are benefits significant? (Controversial.) – think about “nudge theory” and other “non-rational” models of behavior.
- May get buy-in only from people who would exercise anyhow. These may be the main users and so no real measurable benefits for individuals’ health outcomes.
- Might make some people nervous due to lack of understanding of results. (e.g., like a prostate-specific antigen or PSA test.)
- Some people may become obsessive-compulsive about meeting self-imposed or external targets.
- Privacy concerns. Who will “own” the information? Can it be sold? More comprehensive consent requirements make people less willing to participate in programs that involve providing personal data.

Issues about data security

- Hacking is a big challenge. Secure servers are never 100% secure.
- Improving technical side of security can have offsetting effects on human behavior leading to reduced security.
- Possible disgruntled employees may leak information.
- Organizational failure. (NHS example, 2014 report that Royal Free London National Health Service A&E department transferred 1.6 million patient records to Google's DeepMind with sufficiently fine information that many individuals could have been identified. It was found that the four data protection principles were breached.)

Lessons from research on information security

- Having highly trained and – more importantly – highly paid employees improves data security.
- Surprisingly, some empirical evidence finds that the use of encryption software does not reduce the instances of data loss but rather increases the risk.
- Ponemon (2009) found that 88% of data breaches in 2008 could be traced back to insider negligence.
- Miller and Tucker (2017) discuss finding little correlation between data loss and the enactment of data-breach notification laws.

Potential value through insurance market underwriting

- What are the problems of moral hazard and adverse selection?
- Note that moral hazard (hidden action/behaviour) and adverse selection (hidden type – immutable characteristics) can compromise insurance market efficiency. Both problems are often simultaneously present.
- Eliminating moral hazard or adverse selection traditionally thought to improve insurance market functioning and may lower average price of insurance to consumers.
- Avoiding adverse selection may improve insurance market profits. There is a sense in which this is also good for consumers.

Uses for insurers beyond (or instead of) underwriting

- Could be used for marketing – e.g., provide an app to consumers for personal use with no tie to insurance premiums or discounts.

- Insurers could use this information to improve future underwriting through linking tracking data to personal (immutable) characteristics correlated to tracking information.

- Insurers could use past tracking information of clients to tailor contract renewal terms and decision to renew.

BUT!

- If some insurers are better at strategic design of contracts based on information from wearables, then other insurers could suffer.

- Use of information from wearables can be argued to increase discrimination and may worsen inequality. (Think about people with physical disabilities.)

- Negative externalities for those consumers who prefer **NOT** to allow monitoring of activities associated with wearables due to their high privacy costs. Nonparticipants or those who score poorly are more likely to end up with higher costs of insurance or lower rewards from employers.

Broader Potential Societal Benefits

- Data from wearables and telematics could lead to better understanding of health benefits of different behaviours. (Consider 23andme.)

- Wellness programs designed to effectively utilize wearables could lead to a cultural shift with health and wellness benefits, possibly even changing attitudes about privacy to such information. (Are millennials less concerned with privacy?)

- Integration of information from wearables with biobanks that includes genetic information could also lead to better understanding of health regarding interaction of genes and environment (e.g., genetic predisposition to diabetes type II and exercise).

- But beware of the “big data” problem involved with such research!

Existing Regulatory Agencies / Legislation

- Canada (Office of the Privacy Commissioner of Canada)
  PIPEDA: The Personal Information Protection and Electronic Documents Act

- States have wide variety of privacy laws. (See Pritts, et al., 2002, "The State of Health Privacy: A Survey of State Health Privacy Statutes." Technical Report, 2nd ed., Health Privacy Project, Institute for Health care Research and Policy, Georgetown University.)

- HIPPA, 1996: **Health Insurance Portability and Accountability Act**

- Patient Protection and Affordable Care Act

Challenges for Regulation

- Is the information from wearables sufficiently accurate to warrant its use for underwriting, etc.?
- Should restrictions on its uses be set and what form should they take?
- Privacy issues and data breaches pose serious challenges.
- EXAMPLE: Exceptions or a “Safe Harbor” for encryption are at the heart of recent modifications to HIPAA (i.e., excepting the need to notify affected parties and the federal government in the event of an electronic personal health if data is encrypted). But encryption may actually weaken security due to impact on human effort.

Further Questions

- Will each wellness plan (or insurer) adopt a standard for users' health tracking devices? Or will individuals be able to choose a different quality device? (Should this be regulated?)

- Will employers some day require access to historical tracking data of job applicants and select those with better results? (Should this be regulated?)

- Will individuals facing some disability – mild to moderate to severe – be required to meet the same targets for rewards or premium discounts? (Should this be regulated?)