



Since the last decade, wearable technology moved from developers' drawing boards to stores, with barely a whisper of disquiet about data privacy. Yet, the implications for data privacy should not be underestimated. There is growing interest in the potential of wearables to mitigate, treat or prevent chronic conditions which put a strain on health economies--ranging from chronic back pain or physical stress injuries to mental health issues like work-related stress. EuroScientist investigates how the latest regulatory framework could secure people's privacy as they strive to prevent chronic conditions through wearable technology.

Chronic disease prevention using wearable tech: not that simple



Wearables could help prevent chronic illness but people's privacy could be at stakes

Since the launch of the Apple-Nike Fitbit in 2009 to the first consumer smart watches in 2012, common features such as activity tracking and heart rate monitoring have been used without question as tools to understand our individual physical performance. The technology taps the trend commonly referred to as [the quantified self](#).

But what happens when the performance of groups of individuals--a workforce--is captured by wearable tech to address the causes and symptoms of chronic health conditions and sick leave? Here, *EuroScientist* investigates the balance between personal privacy and the potential of wearables to

reduce the burden of chronic illnesses on the public health purse.

Disease management and productivity

To what extent can wearables play a role in tackling chronic illness? "Chronic disease management and primary prevention are clearly the area where wearables have a big role," said Ilkka Korhonen, professor of signal processing and leader of the personal health informatics research group at Tampere University of Technology in Finland.

For instance, "think about the management of diabetes, blood pressure or hypertension and similar conditions. Activity trackers are already used quite widely in diabetes management, Korhonen notes, adding: "of course, blood glucose meters are also available but they are not wearables as such; these are more like pocket devices. For cardiovascular diseases in general, people are quite often advised to use heart rate monitors for exercise to help manage the condition."

As a result, wearables carry the twin potential of improving workplace health as well as improving productivity. These are attractive objectives for governments, public health services and employers alike from a time, cost and resourcing perspective.

Wearables used in the workplace, at this stage, have primarily been geared to improve productivity, according to Korhonen. He notes: "It's good to bear in mind that employee productivity comes from two factors. The first is prevention of absenteeism. The second is a reduction of presentism: when you are in the workplace but because of your physical condition, you are suffering from reduced productivity. It's been pretty well shown that employees with good physical condition are usually more productive because they are in better health."

Illness prevention

A [2014 study](#) co-authored by academics from Goldsmiths, University of London, UK, examined the use of brain activity sensors, motion monitors and posture coaches in office environments.

"Just as the early adopters of wearable technology in sports science were able to gain quite significant advantages on the track and field, we're going to see companies that adopt these technologies in interesting and innovative ways, gain huge advantages as a result," says study author Chris Brauer, director of innovation and senior lecturer at the Institute for Management Studies at Goldsmiths. "These may be companies that engage in a transparent way with their workforce, or maybe not," he adds, "There's definitely a social contract idea between the employer and the workforce that needs to be worked out."

The [use of wearables in the workplace is growing](#) and posing new ethical and regulatory questions about the balance between workforce health and efficiency, versus individual privacy and employee rights.

One key element in the debate is how wearables can reduce the causes of chronic conditions that lead to short and long-term employee sick leave, as well as reduce workplace accidents.

Almost half of all employee absences, lasting three days or more across the European Union, are due to potentially avoidable work-related musculoskeletal disorders (MSDs), [according to the UK think tank, The Work Foundation](#).

The direct and indirect costs are estimated at €240 billion each year—representing up to 2% of GDP across the EU member states. [One EU study](#) reported the increasing cost to the public purse from MSDs in Austria, Germany and France in particular. According to the study, in France alone, an estimated seven million workdays are lost due to MSD-related sickness absence.

The perceived commercial opportunity around workplace health is fueling the growth of start-up tech companies using wearables to [treat and prevent chronic conditions](#), including MSDs. The players range from [Quell](#) and [Thimble](#), which use low-voltage current to stimulate back muscles to alleviate back pain, to [Lumo](#), which monitors movement, sleep patterns and vibrates to alert users when posture is poor and when there is increased risk of strain injuries.

Privacy regulation

However, as wearables move from lifestyle apps to workplace monitors—be it to mitigate employee absence and improve health or drive employee efficiency and productivity—key questions remain to be answered. Who owns the data? What are the limits on how it can be used? The problem is that disclosure, storage and usage requirements for app developers, public and private sector organisations around wearable tech has been unclear since the beginning.

Partly, this is due to different data privacy rules across the EU member states. Partly, [as the European Commission \(EC\) has conceded](#), this is due to uncertainty about whether or not data from wearable fitness trackers or heart-rate has the same legal status as data from medical equipment.

In principle, the announcement of a European Commission, European Parliament and European Council [agreement on an EU-wide data protection policy](#) in December 2015 brought good news. It should bring consistency to how consumers, employers and app developers approach wearable technology. Nevertheless, the policy is unlikely to come into force before 2018.

Yet, some legal experts have warned that if the effect of the agreement is to classify consumer wearable data in the same way as medical data, [innovation in health technology may be stifled](#).

Staff at Stockholm's Epicenter innovation lab are taking a bolder step to try to shape innovation around personal tech in the workplace and inform policymakers about the implications for digital privacy. Instead of wearing the technology, they have volunteered to implant an RFID (radio-frequency identification) chip under the skin of one hand, testing its possible applications as an alternative to security keys or even making the office photocopiers work.

"I am deeply worried about our lack of privacy in the digital sphere," said Hannes Sjoblad, chief disruption officer at the Epicenter. "That said, we are the experimenters who look for the solutions of tomorrow. We serve a role in society by experimenting on the fringes of what is possible. We also try to do this in an open fashion and share insights. I see that as our contribution."

Researchers working in the field of digital health data seem more certain of the fundamental principles, however. "My own perspective--perhaps a little bit of a European perspective--is that people should own their own data," added Korhonen. "For example, in the case of corporate wellness, employers should never have access to the data of an individual employee under any conditions. If that started to happen, there are ethical concerns."

Question of interpretation

One of the inevitable challenges of wearable technology, Korhonen notes, is accurate interpretation of data, particularly around individual health. "When we started in the 1990s in this kind of research, we thought that it would be about people having sensors in their homes and sending data in for interpretation," Korhonen added.

"Quite soon we understood that medical professionals were interpreting data without talking to people. So while medical professionals are the best experts for the health side of this, people themselves are the best experts in their daily lifestyle. The best approach is to have a partnership between these two sides."

Yet if a medical practitioner has the potential to misread data from wearable technology, what is the risk of a manager misinterpreting data from employees in the same way?

Ongoing monitoring

The privacy issues around wearables and promoting better health are compounded by the need for ongoing monitoring and use. The benefits of the technology are in recurrent and consistent use; to monitor trend data and as ongoing treatment. The consequence is the creation over time of an archive of personal health data.

A Pennsylvania State University and University of California Davis [study published in 2016](#) explored how wearables and other mobile health apps could promote physical activity and encourage positive behaviour change among users.

The researchers noted that "low re-use rates" over time--as individual's interest in the technology waned--was a key barrier to overcome in the design and promotion of wearables, if health benefits were to be achieved. The study also noted the development of "mHealth technology to manage chronic conditions and improve wellness is becoming ubiquitous. Yet this development is occurring in large part independent of the health care system."

Echoing the view of Korhonen, the US study suggested that the potential of wearables to improve health and prevent chronic illness needed a partnership between healthcare practitioners and individuals. The study concludes: "at a basic level, the mHealth tools offered to users should be intuitive, integrated with existing technology, and should allow the user to control what data are collected and shared."

[Paul Hill](#)

Copyright: [Jacob Lund via Shutterstock](#)