Wearable technology and the corporate wellness strategy

Katie McMullan, Associate at Hogan Lovells International LLP, ***looks at the issues with health monitoring devices, and advises on how best to navigate them***

Many employers are considering the role that wearable technologies, including Apple Watch and fitness trackers like Fitbit or Jawbone can play in their corporate wellness programmes. The potential benefits are definitely attractive — incentivising employees to be more physically active could result in a healthier, more engaged, productive workforce and lower insurance premiums.

Using the health monitoring capabilities of these devices may also be a desirable way to help employers to understand if an employee is really unwell when they phone in sick. The opportunities presented by this particular use have not escaped the attention of wearable tech manufacturers — one of FitBit's 5 strategic goals as noted in its IPO prospectus is to 'further penetrate the corporate wellness market'.

Given the potential for vast amounts of data to be collected, and data going well beyond employees' professional lives at that, employers wishing to use wearable technology as part of their corporate wellness programmes will need to take measures to show that they have carefully considered the privacy rights of their staff. This article analyses some of the main privacy issues, and suggests how these may be navigated.

Transparency

Employers should think carefully about the best way to provide suitable, prominent and meaningful information to employees about how data collected from wearable technology in this context will be used.

Burying a notice or consent mechanism within an employee privacy policy will not meet the required standards, so careful attention must be paid to transparency to get the right messages across.

Legal basis for the use of data

Employers may wish to rely on employee consent as a way to legitimise use of devices, which may well be possible if the organisation makes participation in the programme using wearable technology completely voluntary.

For any such consent to be considered valid, it must be 'freely given' (as well as specific and informed), which will not be possible where staff feel obliged or compelled to sign up (for example, if it would negatively impact their pay or bonus if they decided not to).

It may also be possible to rely on the employer's 'legitimate interests', provided the interests it is protecting are not outweighed by the privacy rights of its employees or unwarranted as a result of prejudice to them, for example if the proposed use intrudes into the expected employment relationship from the point of view of the employee.

Purpose limitation

It will be important to clearly decide the purposes for which an employer is using data collected using wearable technology to ensure that these potential uses can be considered and built into privacy practices from the outset.

Going forward, operational and technical measures should be put in place to ensure that these purposes are not expanded on except in very specific and limited circumstances (and typically following a new data protection impact assessment).

Proportionality

Employers wishing to use wearable technology as part of their corporate wellness programmes need to work with lawyers, Privacy Officers and regulators to develop a sense for where the 'creepy line' is. Particular care will need to be taken to limit the use of employee data to the specific purposes of the programme without making such use 'excessive'.

Data accuracy

One benefit of wearable technology, which assists greatly in the accuracy of information, is that data collection is automated.

However, employers need to be realistic about the current limitations of wearable technology. Programmes and potential

(Continued on page 10)

(Continued from page 9)

uses of data collected will need to be properly calibrated to take account of the possibility for an employee to 'skew' the data collection (for example, by sharing the wearable with a younger, more active family member or by holding and shaking the device to simulate activity).

Retention

Employers need to compile and document a list of business reasons to keep the data collected by wearable technologies. This process should reveal which data are really necessary. Based on this analysis, employers should implement data retention standards and a deletion procedure for all data collected in the context of its wellness programme.

The rights of individuals

Employees have certain rights to access their own personal information and seek correction or object to its use by their employer. Therefore, employers need to prepare and implement internal policies that describe the appropriate actions to be taken in the event of any such request to assist staff in handling data protection requests.

Security

Given the potentially vast amount of data involved and the serious harm that would be caused in the event that the data are compromised (particularly if health related data are collected), employers need to give serious regard to ensuring that appropriate and robust security measures are in place ensuring that data are kept appropriately secure.

"Employers wishing to use wearable technology as part of their corporate wellness programmes need to work with lawyers, privacy officers and regulators to develop a sense for where the 'creepy line' is. Particular care will need to be taken to limit the use employee data for the specific purposes of the programme without making such use 'excessive'."

Third parties/ vendors

If employers will engage a third party vendor to process data on their behalf in this context, they must also ensure that the usual written data processing agreements are in place and undertake appropriate due diligence to ensure the suitability of the relevant vendor/s.

International data flows

Where data are transferred from within the EEA to outside the EEA, employers must also ensure that the rules restricting international data transfers (such as Safe Harbor, Binding Corporate Rules or using the EU Model Clauses) are in place.

Future-proofing privacy

Under the new draft data protection Regulation, businesses will be required to carry out Data Protection Impact Assessments for processing operations which present specific risks to individuals due to the nature or scope of the processing operation. The use of wearable technology in an employment context will almost certainly come within this requirement.

If your organisation is considering deploying wearable technology as part of its corporate wellness programme, it would be highly advisable to carry out a Data Protection Impact Assessment before doing so, to future-proof your privacy practices in advance of the new regime.

Katie McMullan
Hogan Lovells International LLP
katie.mcmullan@hoganlovells.com