Global Counsel

NHS and Amazon: is privacy being sold down the river?

Blog post by Practice Lead Tom Smith, 10 July 2019

The decision by the NHS to share basic health assessment information with Amazon for use through its Alexa virtual assistant service may appear an effective way of reducing pressure on primary care services, but a question arises of what Amazon will do with all the ostensibly valuable data it gleans, and whether this will be shared with the NHS. Against a backdrop of a wider debate on 'surveillance capitalism' and the relationship between tech giants and individual privacy, a more focused debate is already underway in the UK on the outlook for the use of data related to healthcare. For policymakers, this can be reduced to two main challenges. Firstly, how to protect patient privacy and encourage transparency. Secondly, how to share the rewards from what is hopefully a productive exploitation of a seemingly public good. Policymakers need to respond to both if an effective 'social contract' can be crafted to underpin a global market that could be worth £50-70 bn by 2025.

For Amazon's participation in NHS provision to be considered legitimate, the agreement made between the two organisations needs to satisfy a range of tests. On privacy and security, Alexa users must be confident that they know what happens to their health data, what it is used for and how they can control it. On efficacy it could be argued that Alexa is acting as a medical device and should be regulated as such with independent research to assess safety and patient outcomes. And on fiduciary responsibility, Amazon has to avoid the perception that it is 'profiteering' by engaging with the NHS. The NHS, for its part, needs to avoid the accusation that it has given away the right to collect a valuable data asset without any benefit accruing as a public good. Should all of these tests be met, Alexa (and other personal assistants) could prove beneficial in acting as an effective triage tool, but more importantly as a connected homes tool to help a wide range of groups from those with visual impairments to those with dementia.

In the UK, the National Data Guardian, Fiona Caldicott, has just published research showing that while most people are supportive of the sharing of anonymised health data in return for quicker and cheaper access to treatments (and even supportive of profitmaking), the public debate is still at an embryonic stage. Caldicott's primary conclusion is that there needs to be a broader conversation. Nonetheless, it was clear that the public wanted the gain to be shared equitably between patients, the NHS and researchers. This is relatively good news for Amazon but depends a lot on how transparent they are prepared to be on their use of user data gathered through Alexa interactions.

A prerequisite for designing a meaningful framework for reaping the dividends from health data is drawing out what exactly researchers, both profit and non-profit, use data for; so far Amazon has indicated that it will not share the data with third parties or perform its own analysis, which may make this a moot point but generates a substantial opportunity cost. The Wellcome Trust, amongst others, has made substantial progress in expanding this debate at a national and general level. What is arguably missing is consumers' awareness of specific data being collected about them, who exactly is using it and for what purpose. How easy is it, for example, for a Fitbit user to see the tangible utilisation of their data should they choose to share it with researchers? This ambiguity could be resolved through an

evolution of the regulatory framework by specifying in law exactly how health data should be collected and used.

The debate in the US is arguably more advanced, albeit driven more by the sensitivities over the interaction between data collection and the cost of health insurance premiums, it has been stimulated by a booming market in data, such as pregnancy app Ovia's sharing of aggregated data with employers. Arguing that sector-agnostic frameworks such as GDPR or the California Consumer Privacy Act do not go far enough regarding health data, especially on the ethical, downstream use of data, legislators have introduced a bill with bipartisan support seeking to strengthen regulations for data collected through wearables, health apps and other online sources. If successful, the bill would prompt regulators to standardise consent procedures, give individuals greater control over the use of their data and substantially limit the scope for third party re-sale or re-processing of data. Both consumers and industry in the UK and EU could also benefit from such clarity.

Provisions of the proposed Protecting Personal Health Data Act include:

- Uniform standards for consent related to the handling of genetic, biometric and personal health data
- Minimum standards of security
- Standards for the de-identification of personal health data
- Limitations on the collection, use and disclosure of health data
- Standardise the process by which regulators and industry discuss rule evolution
- Clear process to withdraw consent
- Right to view, delete and amend any data collected, analysed or used

While private medical insurance is used by a minority in the UK, the growing proclivity for wearables and digital health treatments raises equally serious regulatory questions. While apps and wearables generally comply with the GDPR provisions for consent around sensitive personal data, big questions remain. In practical terms, the regulatory framework as it stands does not aid consumers in their awareness of the extent of personal data being collected, what uses it is being put to and what end products and services it is underpinning - information that, more often than not, would encourage individuals to share their data more.

Resolving these questions in the regulatory framework leads to more complex considerations once metadata has been collated, new products, algorithms and services developed. Researchers, clinicians and the public will rely, to some extent, on the veracity and accuracy of this metadata but where does the consent for use of metadata and liability, should it lead to poor outcomes, lie? Complex questions of choice and consent will arise, but it is not clear in which part of the ecosystem this debate will take place, or whether it could democratise the health and life sciences industry. This could lead, for example, to individuals opting out of the use of their data where animal testing is used, or where state actors they disapprove of are involved.

In some jurisdictions, concerns are such that some parts of the market have been prohibited, such as the sale of smartwatches to children in Germany. The response is unlikely to be as drastic in the UK but there is clearly a gap in the regulatory framework that Caldicott and others such as the Understanding Patient Data initiative are seeking to fill. An end state where educated consumers have control over how their data is collected, stored and processed, and how they can benefit personally from it, outlined in a standardised and transparent way, seems a reasonable goal. In the meantime, the risk for Amazon, and indirectly for the health-internet-of-things drive from the NHS, is that public suspicion over the end use of health data stymies attempts to roll out tech-enabled enhancements.