eHealthlaw&policy

The monthly journal for the connected health industry

VOLUME 03 ISSUE 01 JANUARY 2016 WWW.E-COMLAW.COM

NIS Directive broadly positive for EU eHealth

The proposed Network and Information Security ('NIS') Directive, which was informally agreed by the European Parliament and Council on 7 December, "is broadly speaking, a positive development for eHealth in the EU," says Brian Kelly, Associate at Covington & Burling LLP.

The Directive, which is the first piece of legislation on cyber security in Europe, will require 'operators of essential services,' which identifies operators in healthcare settings and entities involved in the provision of healthcare as falling within the scope of that definition, to adopt certain cyber security measures and notify serious cyber security incidents to the national competent authority.

For healthcare and other critical sectors, Member States will be required to identify the 'operators of essential services.' "It will be important to see how Member States distinguish between health services they expect to comply and those who do not," adds Kelly. "It seems likely that web-based IT systems of hospitals and clinics will have to comply, but the extent to which other eHealth operators may be subject to the Directive is less certain."

IN THIS ISSUE

Data Protection EU General Data Protection Regulation **03**

Medical Devices MDR & IVDR EU update **06**

Workplace Wellness US workplace wellness schemes & eHealth **10**

Collaboration Italy-US Congress report **13**

Case Law NHS data-sharing case verdict **14**

Code drafted to assist mHealth app developers with privacy law

The first draft of a privacy Code of Conduct for mHealth apps was presented at a meeting organised by DG Connect and the European Commission in Brussels on 7 December. The Code is intended for use by app developers and focuses on safeguarding the privacy of data that is collected by mHealth apps, in order to guide developers' understanding of relevant data protection law.

"Data protection is a very important consideration, especially now that the General Data Protection Regulation has cleared its trilogue," says Erik Vollebregt, Partner at Axon Lawyers. "Given the Dutch DPA's recent decision in the Nike Fuel platform case it looks like the scope of application of the special regime for data concerning health has been extended considerably and a lot more companies need to consider the principles set out in the Code."

The draft Code covers topics such as the principles developers should consider prior to making an mHealth app available, for instance purpose limitation, as well as guidance on obtaining consent and on data retention. The Code also provides a definition of 'data concerning health' as 'any data related to the physical or mental health of an individual, or to the provision of health services to the individual.' Not necessarily included under this is lifestyle data for example that relates to a person's habits and behaviour but without a clear link to a person's health status. "The Code currently does not apply to lifestyle data apps and some will view this as a missed opportunity," says Wim Nauwelaerts, Partner at Hunton & Williams. "However, by narrowing its scope, the Code emphasises the distinction between apps that collect health data and those that focus on lifestyle data. That distinction is crucial, because health data is subject to heightened protection under EU data protection law."

Mónica Oliveira Costa, Partner at Coelho Ribeiro & Associados, suggests that "Two of the key challenges ahead are adherence and enforcement because without them the Code will not survive. Thus, these are topics that should be focused on for the Code to be implemented successfully and for it to contribute to greater legal certainty for the mHealth industry." Vollebregt adds that "there is the challenge of having the Code blessed by the Article 29 Working Party ('WP29'), one of the goals of the Commission. But we have seen with the C-SIG code, which also had that goal, that WP29 is critical and the process may take years."

Class action filed against Fitbit in the US over accuracy claims

Three plaintiffs representing a class of customers who have purchased Fitbit Charge HR or Fitbit Surge heart rate trackers filed a lawsuit in a California court on 5 January, alleging the trackers 'consistently mis-record heart rates by a very significant margin' and that Fitbit has defrauded consumers.

The plaintiffs claim to have performed testing to substantiate their complaints. Fitbit has disputed the allegations and noted in a statement to the MobiHealthNews website that its trackers "are not intended to be scientific or medical devices."

"While the plaintiffs here claim some risk, the Food and Drug Administration ('FDA') does not seem interested, at least historically, in pursuing what is advertised as consumer grade, not medical device grade, products," explains Bradley Merrill Thompson, Member at Epstein Becker Green. "Fitbit did seem to be making bold claims that its products were comparable to chest-worn monitors. So if a company gets too aggressive in this space, the FDA might well step in."

Meanwhile, the Federal Trade Commission ('FTC') settled with Lumosity, a software developer, after alleging that Lumosity deceived consumers via unfounded claims that its games could, *inter alia*, reduce or delay cognitive impairment associated with age. "The FTC expects companies to have data to substantiate their claims," says Yarmela Pavlovic, Partner at Hogan Lovells. "As this industry increases in size, I expect the FTC to continue to increase its enforcement oversight."