NHS

NHS app storing facial verification data via contract with firm linked to Tory donors

Rob Davies

@ByRobDavies

Wed 15 Sep 2021 06.00 BST

The NHS app is collecting and storing facial verification data from citizens in England in a process which has fuelled concerns about transparency and accountability.

The data collection is taking place under a contract with a company linked to Tory donors called iProov, awarded by NHS Digital in 2019, which has yet to be published on the government website.

Privacy campaigners say the opacity of the relationship between London-based iProov and the government raises questions about how securely the information is held, with one saying they were “deeply concerned” about the secrecy surrounding the use of data.

An NHS spokesperson confirmed law enforcement bodies were able to request data, but that a special panel reviewed such requests, taking into account the health

service's duty of confidence.

The number of users reached 10m this year after the app was adapted to act as a Covid-19 passport. It is used to access medical records and book GP appointments, as well as obtain certificates which prove an individual's vaccine status for overseas travel, or for entry to events such as football matches. The number of users has grown by six million since the Covid pass was introduced in mid-May. The app is separate from the official NHS Covid-19 app, which acts as a contact tracer.

The app asks some users for video facial verification by default, although it is possible to opt out of the process.

The process involves new users recording a video of their face. The video is sent to iProov which compares the facial data with anonymised photo IDs already held by the government. Its Flashmark software beams a one-off sequence of colours at the user's face, through their phone, to ensure they are genuinely present during the verification process.

The app also asks users to upload their date of birth, postcode, phone number and a photo of either their passport or driving licence during the sign-up process. Only a photo clipped from the ID document is supplied to IProov.

Both iProov and NHS Digital stressed that app users' biometric data is anonymised and guarded via the best possible security protection, audited by the NHS. IProov insists its customers implement a "privacy firewall" to ensure it has no visibility whatsoever of the identity of the people it verifies, apart from their faces, which is the service it provides.

However, NHS Digital said it had not published its contract with iProov "for security reasons". It also cited security as a reason for not publishing a data protection impact assessment (DPIA) of the NHS app, the document that explains how individuals' information will be used, stored and protected.

IProov said it could not disclose how long it holds facial data for. The NHS said the information is "not stored for longer than is necessary under the contract".

One expert in surveillance law, who asked not to be named, said such information was likely to be desirable to UK and foreign intelligence services.

"If GCHQ acquired it and it was of use, the likely position is that they would share that with the [US] National Security Agency," they said.

Jake Hurfurt, head of research and investigations at civil liberties group Big Brother Watch, said: "We're deeply concerned by the secrecy surrounding facial verification

and data flows in the NHS app, particularly given the involvement of a private company.

“It raises questions about how private and secure anyone’s information is when using facial verification and the NHS login. Anyone who sends personal information to a private company, at the encouragement of the NHS, has a right to know exactly what happens to their data.”

Dr Stephanie Hare, author of Technology Ethics, said: “Transparency, explainability and accountability are the holy trinity of technology ethics and they fall down on every one of them.”

London-based iProov has previously won contracts with HM Revenue & Customs and worked on the Home Office’s “settled status” Brexit scheme for EU citizens who wish to remain in the UK.

It is also linked to Conservative donors. The company has received financial backing from private equity group JRJ, which has a seat on the board after investing in 2015 and 2019, the year iProov won its first NHS contract.

JRJ counts two Tory party benefactors among its three partners. One, the former Lehman Brothers executive Jeremy Isaacs, made 26 donations totalling £661,500 to the party and its MPs between June 2006 and February 2021.

His fellow JRJ partner, Roger Nagioff, donated 15 times between May 2004 and February 2020, giving £448,500. JRJ did not return a request for comment but a source familiar with its investment said JRJ owned less than 10% of iProov and had no involvement in the NHS contract.

The iProov board includes data security experts and a veteran of Her Majesty’s Government Communications Centre (HMGCC), which has developed surveillance technology for the government.

Eddie Alleyn, a non-executive director, joined the diplomatic service in 1981 after leaving Oxford University, going on to work at the Ministry of Defence and Foreign Office, where he ran HMGCC.

IProov said: “Mr Alleyn’s role is to bring impartiality and business experience to the board. He is subject to the legal obligations that apply to directors of private companies, as prescribed by the Companies Act 2006. Mr Alleyn has no executive responsibilities and no influence over iProov’s data processing.”

IProov won its contract to provide facial verification software to the NHS amid a drive to digitise the health service.

While the contract hasn't been published, documents on the government's "digital marketplace" website show that it typically charges an annual service fee of up to £1.4m and a cost per user of £1.50.

The NHS said it had secured a discount.

IProov also sells its software to businesses including Eurostar and several banks, as well as to foreign agencies including the US Department of Homeland Security. It does not sell data. It said all of its activities were regulated by GDPR and that UK law protects against it being compelled to release or hand over any user data.

Its founder-boss Andrew Bud has spoken of his desire for facial recognition to be used in more settings in the UK, including on the door of venues such as nightclubs.

Cori Crider, director of Foxglove, a team of lawyers investigating the misuse of technology, said : "So long as this system to log into the NHS app is optional then it may be fine but officials definitely shouldn't be 'nudging' patients to log in with their faces to access healthcare.

"We should all also reflect on whether we're heading towards a world where people have to use their faces just to walk into the supermarket or the pharmacy or the nightclub."

Dr Stephanie Hare said: "Once this stuff is brought in, it's very difficult to get rid of. It's the thin end of the wedge and Covid is an opportunity for companies to get a foothold."

A spokesperson for NHS Digital said: "The NHS app is helping millions of people to quickly and easily access their NHS Covid Pass, and frees up time for GP surgeries by allowing people to book appointments and order repeat prescriptions online.

"We use facial verification software when people decide to use the app to access their confidential patient data, as part of the high-level NHS login identity verification process which is clearly explained to app users.

"This means people using the NHS app can trust that their data will be safe and secure."