Want to see an NHS doctor? Prepare to cough up your data first.

UK patients required to give private companies access to personal information.

Paul Sawers 'TechCrunch'(USA) 18th March 2024[1]
(Lightly edited and with the addition of footnotes by KONP data WG.)

In part due to growing pressure from the government to meet a two-week limit for patient appointments, family doctors - or general practitioners (GPs) as they're known in the U.K. - are turning to third-party software to facilitate appointments and prioritise cases based on urgency. This shift has left patients with no option but to give private companies access to their personal data.

While the UK's National Health Service (NHS) was once a bastion of state-funded care, where an individual's economic disposition had little bearing on their access to medical services, today it's a somewhat different matter - a victim of chronic underfunding and understaffing with record waiting times for routine hospital treatments and working conditions that have led to doctors, nurses and other clinicians striking 'en masse'.

With the government pushing for further privatisation, corporations have been circling for pieces of the billion-dollar health pie. The NHS has struck controversial data-sharing deals with the likes of Google's DeepMind, while a slew of US tech companies including Google, Microsoft, Amazon and Palantir were awarded contracts as part of the NHS's COVID-19 datastore project four years ago.

At the same time, primary care has also been infiltrated, where for many it's now impossible to get so much as a simple appointment at your local surgery without having to divulge personal information to private companies.

There is no singular body that tracks which GP surgeries are using which software, as this type of data is not centralised in that way - NHS England explains that because it is made up of different organisations, they would need to make individual requests to individual GP surgeries or local integrated care boards (ICBs) that make up the NHS throughout the UK to discover the size of the problem. However, research shows that there are a growing number of surgeries that are using private companies to triage primary care appointments - with no way around it.

One such company is 'Klinik[2]', which is now live across 300 NHS GP surgeries, while 'eConsult[3]' is used by 40%, and 'Patchs Health[4]' supports over 10 million NHS patients.

While IT dependency in the NHS, as with many other sectors today, is becoming the norm, what is new is the growing inability to get the most basic form of NHS

[1] This article was originally aimed at a US audience- search: 'Paul Sawers' 'TechCrunch' ' NHS data' for original article.
[2] https://klinikhealthcaresolutions.com
[3] https://econsult.net
[4] https://patchs.ai

healthcare without giving private companies access to your personal information. And if you don't like it - tough.

Value of data

The more that data spreads, the higher the risk that it will find its way into places where it can be used against patients' interests.[5] And regardless of what promises may exist in privacy policies or are otherwise enshrined in regulation, health data's value is such that the incentives to share it may be too high to resist. For example, a recent investigation by the UK's Observer newspaper[6] revealed how sensitive health information belonging to half-a-million UK citizens that had been donated to UK Biobank for medical research was eventually shared with insurance companies - not quite what the participants had agreed to.

It's difficult to put a precise monetary value on NHS data: Back in 2019 Ernst and Young (EY) says that the potential insights enabled by the vast NHS datasets could be worth as much as £9.6 billion ($12 billion) annually[7]. Indeed, the NHS holds what is deemed by many to be the 'Holy Grail of health data' for various reasons - these includes the comprehensiveness of its national coverage; its longitudinal data collection spanning decades; and the way it has recorded and stored patient records in a consistent, standardised format that makes it easier for machines to analyse.

For instance, doctors codify data using structured clinical terminology (i.e.standardised) such as SNOMED, READ and CTV3. That means that this data is more easily and consistently machine-readable than in other countries where the clinical data is far more in free text, and therefore less easily analysable. This is particularly important as Artificial Intelligence (AI) encroaches further into the healthcare realm, something which the current UK Government very much favours.

Two-week target

When trying to request an online appointment through a GP's website, the author was directed to a third-party system developed by 'Klinik', a Venture Capital-backed Finnish start-up that partners with surgeries to provide "advanced AI triage and patient flow management solutions."

It emerged that the 'Klinik' portal initially asks patients various health-related questions about the nature of their presenting problem, including symptoms. This culminates in a form requesting several further pieces of personal data: name, date-of-birth, mobile number, address, and NHS number.

---

[5] KONP data working group would suggest that this is a bigger issue and is against the public interest generally. For more details see work done jointly with DiU: https://doctorsinunite.com/2024/02/28/intellectual-monopolies-big-tech-and-healthcare/

[6] https://www.theguardian.com/technology/2023/nov/12/private-uk-health-data-donated-medical-research-shared-insurance-companies

[7] https://www.ey.com/en_gl/insights/life-sciences/how-we-can-place-a-value-on-health-care-data#:~:text=The%20curated%20NHS%20data%20set,following%20the%20generation%20of%20insights .

Patients may be provided with an alternative option to make an appointment by using the NHS App system, but the author found that this led to the same place – he was requested to give 'Klinik' access to his personal information.

For those unable or unwilling to use this form, the GP surgery's automated telephone system informs the caller that they could stay on the line to be put directly through to a member of staff - however, the staff member simply manually completes the exact same 'Klinik' form on the patient's behalf.

In other words, there was no way to make an appointment to see a GP without agreeing to give 'Klinik's' system access to your data. And the stated reason was the government's appointment timescale target.

Automated triaging software is designed to ease a burdened NHS healthcare system, guiding patients toward self-help information for minor ailments - it promises to prioritise more urgent cases, saving GPs and their staff from having to converse with every single patient.

The benefits and risks of introducing more automation to clinical decision-making is a discussion in itself, but the big trade-off in the current environment is entrusting personal information to third parties.

'Klinik's' privacy notice confirms that it uses Google Cloud for hosting and storage in the UK, as well as Microsoft for "data reporting" purposes around "pseudonymised personal data"[8]- more specifically it uses 'Power BI'[9] to create reports for its clients "on an aggregated level" that support managerial decision-making.

It seems that monitoring selected aggregated statistics is also necessary on the 'Klinik' side for post-marketing surveillance of the system due to medical device requirements.

On the data privacy and control side, 'Klinik's- policy states that the third-party processors it uses, including Google and Microsoft, are "subject to clear contractual restrictions to only use your personal data as we instruct them to do so, and subject to appropriate security measures"[10].

The spokesperson added:

> 'There are multi-level security layers in place for gaining access and combining different aspects of the data. In that sense, only parties that we allow access to certain data -as per customer request/allowance -can have

[8] For example, given an identifier other than the NHS number for use in analyses etc

[9] https://www.microsoft.com/en-gb/power-platform/products/power-bi/ This is Microsoft's analytic platform- KONP data WG would like to point out that while Microsoft provides analytics, the performance of its own AI algorithm will improve each time the NHS access it with data. This could increase its value in the global market- as 'trained on the NHS database'. This is the same for all the Big Tech platforms.

[10] Note that if analytics are required (and why else do you collect the data?) this does not prevent the performance-and potential financial- benefits any Tech provider may obtain by simply running the NHS data through machine learning AI for the analysis- see footnote [5]. To see how the AI works see: https://learn.microsoft.com/en-us/power-bi/create-reports/sample-artificial-intelligence

> access to it. Google owns the physical premises and hardware where the data is located[11]- we do not have any control for that except contractual agreements. As per Google procedures, however, having physical or technical access does not in any way mean that the data is accessible, as encryption keys and logic for combining scattered data is needed.'

Regardless of what privacy policies might state, and whatever security measures might be in place, history is littered with examples of data being misused or mistreated (deliberately or otherwise). The more third parties that have access to data, the more likely something will go awry somewhere.

Another London-based surgery contacted said that it exclusively uses 'Patchs Health' for appointments, again with no way around it. 'Patchs' is developed by a London-based AI and data science consultancy that used to be called 'Spectra Analytics'[12] and is used for all patients' requests and as a triage tool. The requests can be submitted by patients themselves or reception staff on the patients' behalf if they are unable to do so by asking the few questions either over the phone or in person.

The manager pointed to various reasons why it no longer accepts appointments without using triaging software, including reducing delays in urgent cases, preventing system overcrowding, improving patient safety and satisfaction, and identifying potential red flags through automation.

Data 'controllers'

Legally, GP surgeries are deemed to be the data "controllers"[13], while intermediary software providers are data "processors." And this is a point that 'Klinik' was keen to stress, that patients do not "give away" personal data, insofar as it does not technically own the data - it's more of a custodian.

> "The data is stored pseudonymised and the only way that any data is 'used' is to provide anonymised statistical data to the practices in dashboards, so they can better understand their demand, and to organise themselves. Only if the patient consents can the company use data that is anonymised to improve the calculations of the algorithm. But even then, no personal data is transferred to the company".[10]

Things can get a little more complex though. Digging into 'Patchs' privacy policy, for instance, reveals that it is in fact a data "sub-processor," responsible for developing and maintaining the software. The main data processor contracted to deliver the service is Advanced[14], a private equity-backed company that develops various industry-specific software. The company was acquired and taken private by

[11] European Hyperscale database headquartered in West Dublin, Ireland.
[12] https://patchshealth.com/goodbye-spectra-analytics-hello-patchs-health/
[13] A data controller determines the purposes and means of processing personal data. In other words, the data controller decides the how and why of a data processing operation. A data controller can be a legal person, for example a business, an SME, a public authority, an agency or other body.
[14] https://www.oneadvanced.com A software company Headquartered in a mailbox in Birmingham (but physically in Atlanta, Georgia). Revenue £322m (2023). Primary development function in Bangalore, Karnataka and Baroda, Gujarat, India.

Vista Equity Partners[15] in 2015, with BC Partners buying a portion of it (50%) four years later[16].

This is somewhat like 'Patient Access[17]', which for millions of UK patients serves as the gateway to their local doctor, used to book appointments, order repeat prescriptions, and more. But 'Patient Access' is in fact owned by EMIS Health, which five months ago was acquired by Bordeaux UK Holdings II Limited, an "affiliate" of Optum UK which in turn is a subsidiary of UnitedHealth Group — a $500 billion health and insurance multinational, one of the largest health care companies in the US and the 11th largest company globally by revenue.

On that note, a separate UnitedHealth Group subsidiary Change Healthcare, was recently hit with a ransomware attack, disrupting the US healthcare system and sparking fears that patient data could spill online.

This brings into focus the value of the NHS brand, and how easy it is to inadvertently agree to open-up access to data without really meaning to - the NHS logo can disguise multiple layers of corporate ownership. The 'Patient Access' mobile app and website features the NHS logo prominently, even though it's a private company and is not exclusively used for NHS services[18]. When a patient is making an appointment with their GP, they're not thinking in terms of "how can I protect my data here, and what am I signing up for?"; they are just trying to see their doctor as quickly as possible.

So even if you are happy to embrace technology and open access to a little data, it's difficult to know exactly who you are entrusting it to, and where even it may end up via a complex web of acquisitions and partnerships.

And then there is the issue of liability - who is responsible for safeguarding what, and what happens if things go wrong?

> "In theory, it makes no difference most of the time as the NHS should have done appropriate checks, but in practice it makes no difference until suddenly it does, and the company the NHS thinks it can sue has no assets and claims no responsibility because of legal games." (Sam Smith from health data privacy advocacy group MedConfidential).

Furthermore, while triaging software might help alleviate stress on an over-stretched workforce, it also opens the door to all manner of dubious behaviour, where users inadvertently agree to sharing their data outside the confines of their direct care. By way of example, during 'Patchs' signup you have to opt-in to sharing (anonymised) data for research purposes and must re-enter the system afterwards if you want to opt out. It says:

---

[15] Headquartered in Austin Texas with $100 billions of assets under management.
[16] Barings Capital (BC Partners) headquartered in London with $40 billions of assets under management.
[17] https://www.patientaccess.com currently run by Patient Plaform https://patient.info part of the EMIS Group https://www.emisgroupplc.com
[18] It will also help you to access private local provision of a whole variety of tests and procedures https://www.patientaccess.com/services (very interesting to see what is available)

> “We may share anonymised data from yourself and those you care for with The University of Manchester for research purposes, and with other GPs for monitoring purposes, to make sure ‘Patchs’ is safe and delivering its intended benefits. ‘Anonymised’ means you cannot be identified. At any time, you can stop sharing your anonymised data with The University of Manchester for research purposes on the ‘Data Privacy’ page accessible via the top menu after creating an account and logging in. This will not affect your ability to continue to use ‘Patchs’ to access GP services.”

Separately, the privacy policy also states that it will share patients’ contact details with the University of Manchester “when patients opt-in to sharing them”, however there is no obvious avenue in the registration process either for opting in, or out, of sharing these details with the University of Manchester.

Both ‘Patchs’ and ‘Advanced’ declined to provide comment and clarification.

Sharp transition

None of this is an entirely new phenomenon, as the patient-doctor relationship has become increasingly digitised through the years. But what does seem to have changed is the sharp transition to an extreme where patients can no longer see their doctor without agreeing to use software belonging (directly or indirectly) to billion-dollar corporations and Venture Capital-backed start-ups.

Your own individual experience of this will depend on where you live - some practices still operate more traditional booking processes that do not require giving data over to third-party software providers. But London seems to be more heavily impacted by the shift, and it could be a bellwether for what’s to come elsewhere.

When asked whether it supports patients that are not comfortable giving private companies access to their data to see a doctor, NHS England issued a statement saying that GPs themselves, as the data controllers, are responsible for safeguarding data and must comply with the relevant laws.

> “GPs are responsible for the protection of personal data that identifies patients and must comply with the General Data Protection Regulation (GDPR),” the statement read. “Patients are provided with information by their GP about how their data will be used, who will have access to it, and what security measures are put in place. They can exercise an opt-out to prevent their data being shared for purposes beyond their direct care. Digital platforms must employ secure communication methods to protect personal data used for online consultation, remote triage, appointment booking or other patient services.”

So, there is no automatic expectation that patients can see an NHS GP without giving over data to private companies.