

Collecting GP data - advice for the public

NHS Digital's improved collection of GP data will support vital health and care planning and research. Here we explain how and why your data is being used, and what to do if you don't want your data shared.

medConfidential comments throughout in red

Page contents **as of 22 May 2021**

Why we need your data	1
Why we need a new system	2
How we keep your data secure	2
You can opt out of sharing your data	3
We make it clear how to opt-out	4
If lots of people opt out the data becomes less useful	5
Why we need to collect sensitive data about things like domestic violence and STIs	5
We are not going to sell your data [our emphasis]	6
How we ensure people use the data as promised	7
This is not care.data	7
We have completed a data protection impact assessment	8
Data we will not collect	8

Why we need your data

Patient data is used every day to improve healthcare services through planning and research in England, helping to find better treatments and improve patient care.

It helps to decide what new health and care services are required in a local area, informs clinical guidance and policy, and supports researching and developing cures for serious illnesses, such as heart disease, diabetes, and cancer.

For example, GP data collected as part of the COVID response is being used by the [University of Oxford RECOVERY trial](#), which is looking to find ways to improve the treatment for people with COVID-19.

NHS Digital collects the GP data required for COVID response under extraordinary 'Control Of Patient Information' (COPI) powers that apply during public health emergencies like the

pandemic. That collection is called 'GPES Data for Pandemic Planning and Response' (GDPPR) and if you have not been made aware of it before, you can read about it [here](#).

This new GP data collection, somewhat confusingly called 'GP Data for Planning and Research' (GDPR), is *far bigger* and for a *far wider* range of purposes *far beyond* COVID-related research. Implying by the sole example given for the use of GP data that this new "collect once, use many times" GP data collection is COVID-related is at best cynical – and, given the new programme is being rushed in during the pandemic, more characteristic of Government manipulation than what the public expects of public services like the NHS.

Why we need a new system

Patient data is already being collected to improve health and care services. NHS Digital has collected patient data from general practices using a service called the General Practice Extraction Service (GPES). This system is over 10 years old and now needs to be replaced.

NHS Digital has engaged with doctors, patients, data and governance experts to design a new and improved system to collect data from general practice that:

- reduces work for GPs so they have more time to focus on patient care
- explains clearly how data is used to help patients feel confident and informed
- means data is collected, stored and accessed in a secure and consistent way

medConfidential is in favour of "new and improved systems" for health and social care, but all such improvements must ensure that all uses of patients' and service users' data are consensual, safe, and transparent.

As it currently stands, and as it is being rushed into operation, this new system GDPR does not.

- Unlike many times during COVID, patients across England will not be written to about this scheme to explain what's going to happen and what their choices are
 - Copies of your data will still be sold – i.e. "disseminated" [for payment](#) – not accessed *exclusively* via safe setting (even though NHS Digital has one)
 - You will still not be told how YOUR data is being used, nor who has used it
-

How we keep your data secure

We take our responsibility to safeguard patient data extremely seriously. Data shared by NHS Digital is subject to strict rules around privacy, security and confidentiality and the new service has been designed to the highest standards.

Data will be approved for dissemination by the same body that has been doing so for years; the rules remain largely unchanged since it was formed in 2018. NHS Digital's own audits show [its customers don't follow the rules](#). And, not least because the Government never

brought forward Regulations promised after the care.data and Hospital data scandals of 2014, sanctions are weak and rarely enforced.

We do not collect patients' names or exactly where they live. Any other data that could directly identify someone, for example their NHS number, full postcode and date of birth, is pseudonymised before it leaves their GP practice. This means that this data is replaced with unique codes so patients cannot be directly identified in the data which is shared with us. The data is also securely encrypted.

What NHS Digital doesn't mention is that it holds people's names and addresses already, in its ['Personal Demographics Service'](#). The information collected with every dated medical event about you will allow NHS Digital to individually identify you, or it couldn't link your records. 'Not collecting names and addresses' is a complete straw man; previous schemes such as care.data didn't either - they never needed to.

We would only ever re-identify the data if there was a lawful reason to do so and it would need to be compliant with data protection law. For example, a patient may have agreed to take part in a research project or clinical trial and has already provided consent to their data being shared with the researchers for this purpose.

Consent is only one such reason, and is the most benign. Why did NHS Digital choose not mention that patients' fully-identifiable data can be [\(and is\)](#) disseminated to customers, including other parts of Government, for processing *without* consent? And, [as pointed out already](#), NHS Digital knows some of its customers break the law but still gives them patients' data.

The law allows research projects which need to find volunteers for their research to contact patients directly about taking part in research or a clinical trial if the Health Research Authority has approved the request.

This would also need to be agreed through the [Independent Group Advising on the Release of Data \(IGARD\)](#) and the GP Professional Advisory Group (PAG), which is made up of representatives from the British Medical Association and the Royal College of General Practitioners.

In a "collect once, use many times" world, IGARD (and PAG) are likely to be very busy! What replaces all of the governance and institutional processes that existed when the purpose, specification and sometimes even standards for each and every GP data collection had to be justified individually? Why is it that [institutional customers for patients' data](#) will now run the standards-setting body?

You can opt out of sharing your data

If you do not want your GP to share your identifiable patient data for purposes except for your own care, you can opt-out by registering a [Type 1 Opt-out](#). This prevents your data being shared with NHS Digital if you register your opt-out before **23 June 2021**. You can still register your opt-out at any time after this date and it will prevent any more data being shared with NHS Digital.

...but if you do so after uploads have started it won't have stopped NHS Digital extracting your lifelong GP history, which it will never delete.

You can also register a National Data Opt-out, which will prevent NHS Digital from sharing your identifiable patient data for planning and research purposes. Your individual care will not be affected if you opt-out using either option.

The National Data Opt-out will not stop NHS Digital extracting your lifelong GP history from 1 July 2021, and its own data release registers show [it only respects this opt-out about 20% of the time](#).

Opt-outs (either type) that have been registered in the past will all be fully respected.

We have designed the collection with many safeguards in place to protect the privacy of patients, including removing all personal information that would directly identify patients before data is shared with NHS Digital.

This is false and misleading.

All personal information that could identify patients is not “removed”; identifiers that completely identify patients – like their NHS number – are merely obscured, in a way that NHS Digital can reverse to make them entirely visible again. This process is called ‘pseudonymisation’, and the law is very clear about it: pseudonymised data is still personal data, i.e. information about an identifiable person.

This also doesn't consider medical events that could uniquely identify your record, like your children's birthdays ('maternity events'), accidents that have been reported or details of health episodes you may have posted online.

By putting in place strict governance processes about who can access data and for what reasons, and being transparent about what data is shared and why, the programme aims to make patient data available safely and securely.

So why keep sending out copies? Why not make GP data available *only* via safe setting?

Making data available for research will lead to better:

- NHS services for patients
- treatments
- Medicines

No-one is disputing that research can have positive outcomes. But taking patients' data without properly informing them, and without giving them a fair chance to make a choice undermines the very basis of public trust. If it's so important to get this right, what's the rush?

We make it clear how to opt-out

Although we have designed the collection with privacy protections in place, if patients do still want to opt out, they can. GPs already share data with other organisations for planning and research purposes in accordance with their own data sharing agreements and patients have had the opportunity to opt out of this type of data sharing for several years using the Type 1 Opt Out.

We have provided support and materials to GPs so that they can also let their patients know about the collection. This contains detailed information about it, and the ways that patients can opt out.

In addition to materials for GPs to use, NHS Digital is promoting this new data collection through our website, engagement with media, through our stakeholders and patient groups and on social media channels. We want to raise awareness of the collection and its importance to help the NHS and research take place, but also to provide patients with a choice if they do not want their data to be used in this way.

No-one has written to every patient whose lifelong GP history is about to be copied for onward dissemination to third parties, including commercial interests outside the NHS.

This is neither fair, nor “clear”. Are 50 million patients supposed to visit NHS Digital’s website or Twitter stream over the next 5 weeks?

If lots of people opt out the data becomes less useful

If a large number of people choose to opt out then the data becomes less useful for planning services and conducting research. This is a particular problem if people from certain areas or groups are more likely to opt out. If that happens then services may not reflect the needs of those groups or areas and research may reach misleading conclusions.

[Understanding Patient Data](#) have provided more information on this topic, including specific examples on their website.

If a large number of people opt out, it will be because they do not trust what they are being told – or are concerned at what they haven’t been told – by the Government and NHS bodies. Using implied threats like, “Don’t opt out or your community will suffer” is more the approach of a vested interest than an open and trustworthy, rights-respecting organisation.

Is the [Wellcome Trust’s](#) Understanding Patient Data helping explain to patients how to exercise their right to opt out?

Why we need to collect sensitive data about things like domestic violence and STIs

We need to collect sensitive data to help plan and design services, and research conditions to better support the people affected. For example, we need to collect data about domestic violence to ensure the right local support services are in place. Victims of physical and sexual violence are also more likely to suffer from mental health problems. But without data about these sensitive

events and conditions it is much more difficult to conduct research to provide better services and support.

We respect and protect all the data we collect to the same high standards, but we have also added additional protections as we know how important it is to protect this sensitive data.

This includes going through our [Data Access Request Service \(DARS\)](#) process which means the [Independent Group Advising on the Release of Data \(IGARD\)](#) and a GP Professional Advisory Group (PAG), with representatives from the British Medical Association and the Royal College of General Practitioners, can scrutinise it to ensure the use of that data is absolutely necessary and is legal and appropriate.

The groups and process mentioned above are exactly the same as for other patient data, so where are the “additional protections”? What are the rules about use of this highly sensitive data? Where are these rules published? Who will get access? How will the patients affected be told?

And why, after years of inaction, was the standard which used to define and protect this highly sensitive data “deprecated” in March 2021?

We are not *going* to sell your data *[our emphasis]*

NHS Digital does not sell data. It does however charge those who want to access its data for the costs of making the data available to them. This is because we are not funded centrally to do this. Charges only cover the cost of running the service and means that those organisations who need access to the data bear the costs of this, rather than NHS Digital. We do not make profits from the service.

The data will only be used for health and care planning and research purposes by organisations who have a legal basis and legitimate need to use the data. We publish the details of the data we share on our [data release register](#) so we can be held to account.

We do not allow data to be used solely for commercial purposes.

NHS Digital will not approve requests for data to be used for:

- insurance or marketing purposes
- promoting or selling products or services
- market research
- advertising

...because we *already* do.

NHS Digital provides its many customers with copies of patients' data in a variety of formats. There is a contract between them, i.e. terms and conditions, and money changes hands. To anyone familiar with iTunes or digital transactions, this cannot be described as anything other than a sale.

What NHS Digital chooses to charge, and whether or not it makes a profit on NHS patients' data or enables others to do so, doesn't make the process any less of a sale.

While NHD Digital may not approve requests for the specified activities, it supplies data to 'information intermediaries' which then service clients like pharmaceutical companies, which have marketing divisions. If NHS Digital has the evidence of all the end customers for the data it sends out, it should publish it. If it doesn't, the claims it makes above are all hollow.

How we ensure people use the data as promised

Once data is shared, we carry out [independent audits](#) and, where necessary, post audit reviews to check organisations are using the data for the purposes they said they would, in accordance with the terms and conditions of their data sharing agreements.

Where our data is accessed directly by organisations in our secure research environments, we also carry out audits of who has accessed the data from the organisation to make sure they are authorised users and check how the data has been used in the environment.

This helps to ensure that organisations abide by the terms and conditions set by NHS Digital and data is kept safe and secure.

Any serious breach of our terms and conditions of use would result in the data access being withdrawn and we may report the breach to the Information Commissioners Office (ICO) for investigation.

And yet there *have* been breaches of NHS Digital's terms and conditions, and there *have* been breaches of the law. And yet those customers are *still* receiving data. Why is that?

You can check these assertions against what actually happens at:

<http://theysolditanyway.com/>

This is not care.data

There have been conversations online that have drawn parallels between this programme and something called 'care.data' in 2014. This is not an extension to, or evolution of, that programme.

Patient data is already being collected and used to improve health and care services. This is a new system, designed over the last three years, to improve how data from your GP is shared with organisations involved in the planning of the health and care system, and clinical researchers.

Our processes for accessing data are now very different to those seven years ago when 'care.data' was developed. We uphold the [Caldicott Principles for ethical data sharing](#) and are also bound by data protection laws such as the General Data Protection Regulation (GDPR).

There is also oversight from independent experts on data sharing. This includes the [Independent Group Advising on the Release of Data \(IGARD\)](#) and a GP Professional Advisory Group (PAG), with representatives from the British Medical Association and the Royal College of General Practitioners.

We agree. This 2021 data programme is far bigger, collects far more data, includes details that are far more sensitive and potentially intrusive, and – as if such a thing were possible! – it is being done in a far less fair and transparent way than care.data in 2014. And it's being done in a rush. In a pandemic. While GPs are busy delivering vaccinations, as well as their usual care...

The third Caldicott report was in part prompted by the care.data scandal, and were any NHS body *not* to uphold Dame Fiona's Principles that would be an extraordinary dereliction.

We note it was an independent oversight group (GPES IAG) that spotted issues with care.data in 2013. It was abolished by NHS Digital in 2015.

We have completed a data protection impact assessment

We have carried out a very rigorous and full data protection impact assessment (DPIA) as this is required under the UK General Data Protection Regulation (GDPR) rules.

This is currently going through a final review and assurance process and we will publish the baseline version of it shortly. However, a DPIA is not a static assessment and, therefore, will be reviewed and updated regularly to reflect changes and developments in the service. We will publish updated versions of it from time to time.

The most notable thing about this statement, especially when compared to the one before it, is that *there is no link to a DPIA*.

Why wasn't this published along with everything else on 12 May? NHS Digital says above and elsewhere that it has been developing this programme "over the last three years", so why was the DPIA not ready in time? Have there been problems? Is NHS Digital having to make last-minute changes? What does the Information Commissioner's Office think of it, and when did they see what?

Data we will not collect

We will not collect your entire GP record.

We refer to patients' entire (or lifelong) *GP history*, which is a different thing – namely, every medically relevant event that's been recorded, i.e. coded, in someone's GP record. (It's what a patient would see if they accessed their 'Detailed Care Record' in the NHS App.) The whole GP record contains a whole bunch of other information that's irrelevant, less relevant or which NHS Digital wouldn't be allowed to touch.

We will not collect:

- patient names and full addresses
- **NHS Digital already has a copy of these in the Personal Demographics Service (PDS).**
- written notes (free text) of any consultations or interactions between patients and clinicians
- **You don't need to; you're collecting the coded, dated clinical information from those notes. However, as a "single collection of GP data" how will research which uses those written notes (free text) be supported by NHS Digital? How long will it be until NHS Digital comes back for these written notes?**
- images, letters, videos, or documents
- **As a "single collection of GP data" how will research which uses the information in these be supported by NHS Digital? How long until NHSD comes back for them too?**
- medicines, appointment, or referral data over ten years old
- **Because it wouldn't be lawful (or much point) to collect data that isn't useful to you. Plus, NHS Digital can access referral information from the referral service it runs and the hospital data it already holds.**
- legally restricted data such as IVF treatment or gender reassignment
- **The only clinical data NHS Digital doesn't collect is that which NHS Digital says is explicitly prohibited by law? (Also, to what extent are these restrictions any more real than the norms around the sensitive codes that it is ignoring?)**

We will collect most of the structured and coded elements of the GP record. Find more information on what [structured and coded data means](#).

Ethical behaviour isn't just a matter of following the law. And you can't expect to be trusted if what you do isn't [trustworthy](#).

NHS Digital has made *some* progress since the 'bad old days' of care.data, but – as you can see for yourself from the evasions, half-truths and outright falsehood we have highlighted and evidenced in response to this series of claims – it is nowhere near ready to be taking, irrevocably, a copy of the lifelong GP history of every man, women and child in England who doesn't [opt out in the next four weeks](#).