Public Attitudes on Data Flows Outside NHS Secure Data Environments (2019–2024)

July 2025

Overview of public trust and concerns

Recent public engagement work shows that people generally support the use of health data for public benefit, but trust hinges on strong safeguards. The NHS is one of the most trusted stewards of patient data, especially at a local level (e.g. GP practices and hospitals). However, support quickly falls away if data moves outside the NHS's control or if privacy protections are unclear. Key themes include: ensuring data stays secure within trusted environments, clear pseudonymisation to prevent re-identification, and transparency about who manages data and for what purpose.

Overarching views on sharing data between SDEs

Public support for sharing NHS data between Secure Data Environments is real but not unconditional. It depends on clear demonstration of public benefit, strong technical and ethical safeguards, clear local accountability, transparency about data flows, and meaningful public involvement at every stage.

People generally support sharing NHS health data for research and planning, including between SDEs – but this support is conditional on seeing tangible benefits such as improved care, better treatments, and advances in public health.

The principle of "data for public good" is widely accepted if people understand how their data will be used and protected. People expect data to be kept safe through robust technical measures, strict access controls, and independent oversight – the concept of "Secure Data Environments" aligns well with this, but the public still wants evidence it works in practice.

Many want to know who is accessing data, for what purpose, and that data stays within agreed safeguards. Local control and community oversight also remain important: people want to know local needs and voices shape how their data is used and shared.

Public attitudes turn negative if they believe data could be used for purely commercial gain without benefit to the NHS or the public. There is particular unease about data being linked and shared between environments if this isn't transparent or if there is any risk of misuse by third parties.

The National Data Guardian's work consistently shows that public trust hinges on openness about why data is shared, how it is kept secure, and what accountability exists if things go wrong.

People want regular, clear updates on data flows between SDEs, and evidence that controls and public benefit tests are applied consistently. This should also be communicated clearly, via a trustworthy source, and in language that can be easily understood by the public.

Engagement work highlights that meaningful involvement is key: people expect patient and public voices to shape governance, policy, and real-world decision-making on sharing data between environments. There is support for local and national panels (like Digital Critical Friends or Data Access Committees) to scrutinise how SDEs work together.

Wessex views on sharing data

The following reflects the views of the Wessex public, captured through our Public Panel, deliberative dialogue, engagement with seldom-heard groups, public events, and our Digital Critical Friends.

Trust in the quality of data

When discussing different types of data, people recognised that quality and trust vary depending on what the data is, where it comes from, and how well it is checked. They were concerned about:

- The source of the data (its provenance)
- How rigorous quality checks are
- Whether data could be changed or manipulated for other purposes

Routinely collected NHS data, like test results and blood samples, were generally seen as high quality and 'low risk'. In contrast, sexual health data was viewed as potentially lower quality and more sensitive or 'risky', as people might withhold intimate information from their GP or clinic.

Data collected outside the NHS, for example from commercial wearables, was treated with more scepticism. Some people worried that companies could manipulate this data to serve their own interests rather than the public's. When commercial data is used, the public wants clear reassurance on how its accuracy and quality are checked.

Similar concerns were raised about moving data outside NHS control, for example, to a supercomputer. Participants felt that once data left the SDE, it could be changed or misused if not safeguarded properly.

Sharing data with other SDEs and delegated decision-making

At the start of these conversations, many people assumed NHS data was already shared across NHS organisations, for example, that their hospital records would be accessible regardless of where they received treatment. They broadly supported data sharing between SDEs where the purpose is clear, well defined, and delivers real public benefit to people in Wessex.

There was strong agreement that collaboration between SDEs can be valuable – allowing for larger, richer datasets that can strengthen research quality and scope. However, participants want clarity on how responsibilities and approvals are divided across SDEs. They asked: Will each SDE have separate DAC meetings? Will decisions be delegated – and if so, how are these rules set and influenced by the public?

People also emphasised that the SDE must use its resources appropriately and deliver clear benefits back to the Wessex population. For example, they understood that for rare diseases (like sickle cell conditions), there may not be enough local data to run robust studies, so sharing data across SDEs is necessary. While they support this, they also stressed that only the minimum necessary data should be shared – and that the SDE with the largest or best-quality dataset should lead, provided that robust and consistent safeguards are in place.

When data is shared with other SDEs, participants expect any benefits to be proportional to the effort and volume of data contributed by Wessex. They also want clarity on how learnings and improvements (for example, better data quality or treatment pathways) will be fed back to local services – without creating unnecessary duplication or extra storage costs.

Technical models for moving data across SDEs

Keeping data within Secure Data Environments (SDEs) is seen as a critical safeguard. Public panels responded favourably to the SDE model championed by the NHS Goldacre Review, where researchers come into an NHS-controlled platform to access data rather than data being given away.

Two main technical approaches for cross-SDE data use have been discussed, each with implications for public trust:

- Secure pseudonymised transfers between SDEs: In cases where data must leave one SDE to be used in another, the expectation is that only de-identified (pseudonymised) data would be transferred. Public participants want assurances that any such data movement is tightly controlled – e.g. encrypted in transit, limited to approved recipients, and only between equally secure, accredited environments. They insist that no personally identifiable details travel outside the host environment. Even anonymised data leaving the NHS

makes some people uneasy, so strict governance and clear justification are needed.

- Federated query / in-situ analysis: Many find it more reassuring if data never leaves the original SDE at all. A recent initiative to create a national health data service explicitly promises that de-identified data will be analysed without being exported – instead, queries are sent to where the data resides. This federated approach, where each SDE holds its data locally and only query results or aggregate insights are shared, aligns with public calls to "bring the algorithm to the data" for security. Participants in deliberations viewed the SDE model (which inherently keeps data in one place under NHS oversight) as a key strength that boosts their confidence in data sharing. Knowing that health data remains within secure NHS systems – as opposed to being shared around – addresses fears of uncontrolled dissemination.

In summary, minimising data movement is seen as best practice. Where data must flow outside an SDE, it should be pseudonymised and only go to another trusted environment for clearly defined purposes. Approaches that avoid moving data at all – by using secure linkages or federated analysis – tend to be closer to the ideal from a public trust perspective.

Pseudonymisation Practices and Re-identification Risks

Public participants consistently expect robust pseudonymisation of any patient data used beyond direct care. In dialogues, learning about de-identification measures (removing or coding personal identifiers) provided significant reassurance that individuals "are not exposed to the risk of their personal details being misused or traced back". That said, people also probe the limits of pseudonymisation and worry about how re-identification could occur:

Understanding pseudonymisation

Among the general public there is often confusion and a lack of understanding of terms like anonymisation and pseudonymisation. Once explained, pseudonymisation is welcomed as a key privacy safeguard – effectively a promise that data is only used in coded form. In the NHS England data engagement Cohorts, seeing a concrete example of de-identification (how identifiers are stripped out) helped build trust.

Many were unaware these protections existed. When they learned that research data is de-identified by default, they felt more comfortable sharing data with researchers and across multiple SDEs.

Concerns about re-identification

Despite support for pseudonymisation, participants often ask “could my data be re-identified?” There is recognition that pseudonymised data is not fully anonymous and could, in theory, be linked back with the right key or by cross-referencing unique details. In particular, free-text medical notes and rare combinations of attributes raise red flags – people worry that “you can’t really de-identify the free text… there’s always things that slip through” and rare conditions or demographics are likely to increase the chances of reidentification. These concerns mean pseudonymisation alone is not a cure-all for public trust: the public also expects strict controls on any re-identification process and harsh penalties for misuse.

Handling of pseudonymisation keys

Because re-identification is sometimes necessary (for example, to alert patients to a clinical trial), the public accepts that a secure mechanism (a “key”) can link coded data back to identities. However, they are very clear about who should hold that key. Insights from our Wessex Public Panel in 2024 indicated re-identification should occur only via trusted NHS channels – specifically, a patient’s own clinician or care team within the SDE, not researchers themselves. This implies that any pseudonymisation keys must remain under NHS control (or an independent safe haven acting on the NHS’s behalf).

Participants strongly favoured separation of roles: researchers analyse only pseudonymised data, and if someone needs to be identified, an authorised NHS professional uses the key to do so under tightly governed conditions. The idea of transferring a re-ID key outside the NHS or giving it to non-clinical parties would likely be met with public opposition, as it increases perceived risk. In summary, pseudonymisation keys are seen as the “crown jewels” of patient data – the public expects they will be guarded by a highly trusted party.

Geography, Data Custodians and Sources of Trust

Who holds or manages the data matters greatly to public confidence. Engagement studies from 2020–2024 show a consistent hierarchy of trust: local NHS care providers and NHS institutions overall are trusted far more than other entities with patient data. For example, a National Data Guardian poll in 2020 found 57% would trust the NHS with their data, versus only 32% trusting local authorities (and fewer still trusting private companies). Key expectations and nuances include:

Regional vs. National NHS control

People generally trust the NHS as a whole, but they often relate best to their local NHS services. Many feel data should ideally be managed by NHS bodies – whether regional or national – rather than leaving the NHS. In deliberative workshops, some participants argued for strong local oversight (e.g. each regional SDE having its own Data Access Committee with members reflecting the local population). This was especially important for participants from minority or marginalised communities, who

wanted assurance that decisions about data consider local context and needs. At the same time, others saw advantages in national-level governance for certain decisions to ensure consistency and efficiency – e.g. having a single national approval process for projects using data from multiple regions. The takeaway is that the public want both local sensitivity and national consistency: a network of SDEs where each region has a say, under an umbrella of national standards. Any approach should avoid a perception of distant "centralisation" without local input, as that could erode trust in areas that feel unheard.

Non-NHS environments (ONS, UK Biobank, etc.)

When data moves outside the NHS, trust becomes far more tentative.

Public contributors often are not very familiar with secure research facilities run by other bodies (like the Office for National Statistics Secure Research Service or the UK Biobank's research environment). The instinctive reaction is caution: Is it as safe and are they still accountable to the NHS?

If data from the NHS is to be accessed in a non-NHS setting, people expect the same safeguards and public-benefit focus to apply. In fact, participants frequently demand extra assurances in such cases. For example, deliberations revealed discomfort with even anonymised NHS data being shared with third parties outside the NHS. Many worry that an outside organisation (government agency, university, charity or especially a commercial firm) might misuse the data or not prioritise patient interests. As a result, there is a strong call for transparency and conditional access: any non-NHS body must be fully vetted, data use must be transparent, and there should be legal agreements guaranteeing the data will only be used for agreed purposes and delivering public-benefit in line with the commitments made by the SDEs.

The public is not necessarily opposed to trusted academic or public-sector research environments handling health data – especially if they have a good track record – but that trust has to be earned. Clear communication that, for example, ONS's SRS operates under the "Five Safes" framework and that UK Biobank data use is governed by strict ethics and participant consent, could help. Without such understanding, people lean toward "NHS data should stay in the NHS." Moreover, any hint of commercial exploitation (selling data or private profit from it) significantly heightens public concern.

The NHS vs. private companies

Across all geographies, there is a consistent message that motives matter. The public draws a sharp line between uses that serve the public interest and those that are for profit. While not explicitly asked in every forum about specific companies, participants often volunteer that pharmaceutical and tech companies are less trusted data custodians. The NHS is trusted to have patients' best interests at heart, whereas a private firm is suspected of valuing data for commercial gain. This does

not mean people never want NHS data to be used by private partners, but they insist on robust safeguards and oversight in those partnerships. Any data flows to industry must be governed by enforceable rules (contracts, penalties for misuse, strict approval processes) and ideally be transparent to the public. In essence, trust in data handling is strongly tied to the perceived mission of the holder: an NHS or public institution focused on care and research for society starts with a higher trust baseline than others, and even those others must operate under NHS-led terms to gain acceptance.

Visibility and Understanding: General Public vs. Experienced Contributors

There is a notable gap in awareness and understanding of these issues between the general public and those who have participated in focused public dialogues (such as deliberative dialogue or public panels on data). Most of the general public has low visibility of how health data is handled, and terms like “Secure Data Environment” or “pseudonymisation” are not widely understood in everyday life. Initial reactions from laypeople often include confusion or scepticism, as seen in past studies where people struggled to grasp what de-identified data means or how data flows work. By contrast, members of organised public panels or groups like Wessex’s Digital Critical Friends Group (who engage deeply with NHS data projects) develop a much more nuanced understanding. This difference has several implications:

Need for public education

When the public learn more about data safeguards and see tangible benefits, their support tends to increase. For example, during the NHS England “Data Engagement” deliberations, participants started with significant concern about data sharing and opt-outs. But after 15+ hours of workshops – including expert Q&As on how SDEs secure data – many became more comfortable with data being used, to the point that about a quarter of one cohort even felt opting out should perhaps not be allowed in the interest of the greater good. In Cohort 3 (2025), most participants said that hearing about measures like pseudonymisation and the SDE model gave them confidence that security is taken seriously. Similar results were found from the Wessex Public Panel, which included a core value – Better together – which requires the SDE to consult and educate all communities. This suggests that the wider public might likewise become more trusting if given clear information. Indeed, participants across multiple engagements have recommended awareness campaigns to inform the public about how data is used, the safeguards in place, and the choices people have. They believe transparency and education can pre-empt misunderstanding and “knee-jerk” opt-outs.

Differences in perspective

However, we must be cautious – those who go through detailed deliberations inevitably gain knowledge that sets them apart from the unengaged public. Facilitators note that “the more learning public participants do, the less

representative they may become" of the general population's view. Experienced public contributors often start to think more like data governance advisors, whereas a random person may still feel entirely in the dark about, say, how their GP record might be used for research. The Wessex SDE panel organisers explicitly acknowledged this and stressed the importance of checking deliberative findings against broader public opinion. In practice this means that while an informed group might endorse a federated data solution or trust a specific process, the NHS should ensure these ideas are also tested via surveys or wider engagement to confirm they resonate with the broader public. Inclusion of diverse voices is key – some groups (e.g. those with historical reasons to distrust institutions, or with lower digital literacy) may not participate in workshops but still need their perspectives understood.

Experienced public contributors as champions

Those public members who have engaged deeply can be valuable allies in shaping and communicating policy. Often called "critical friends", they bring a lay perspective informed by training. Bridging the gap between experts and the public, they tend to emphasise the same principles repeatedly: public benefit, security, transparency, and accountability. For example, public contributors involved in data panels have strongly advocated for ongoing transparency (like a "data use transparency hub") and independent audits to keep systems honest. They also understand the complexity better, which leads to conditional support: yes, support data sharing, if it stays in secure environments, if it's pseudonymised, if misuse is punished, and so on. These nuanced positions are a step beyond the simpler "just don't misuse my data" stance of the general public, and they help the NHS identify what safeguards to reinforce. Engaged contributors also frequently highlight the importance of communicating these nuances back out to the wider community, essentially saying: we can accept this, but only if you clearly explain it to everyone and keep listening to public feedback. This creates a virtuous circle where informed public voices help design better policy, and that policy in turn is explained to increase general public understanding.

Conclusion

Public attitudes from 2019–2024 show cautious support for health data sharing beyond direct care, conditional on keeping data safe within trusted systems and ensuring public benefits. People want their NHS data to be used to improve health and services, but not at the expense of privacy or trust.

The NHS's move toward Secure Data Environments and tightly governed data flows is broadly in line with what the public expects: an approach where data is only accessed under strict controls, preferably without leaving the security of the NHS. Pseudonymisation is a cornerstone of acceptability, but it must be done in a transparent way with clear rules about who can ever "unlock" the data.

There remain gaps in awareness – many citizens still have limited visibility of these new data safeguards – so continuing to build public literacy and involve people in

governance is crucial. Importantly, trust is fragile: it hinges on both the reality and perception that data is handled responsibly. Regional NHS bodies, national agencies, and even non-NHS partners like ONS must work together to uphold consistent high standards, as any breach or misuse could undermine the social licence to use data.

By addressing public concerns – keeping data in secure environments, using federated analyses, rigorously pseudonymising data, restricting re-identification, and involving the public in oversight – the NHS can maintain and grow the public's trust that health data is used safely and for good purpose.

Sources:

Recent public engagement reports and literature (2020–2025), including the Wessex NHS SDE Public Panel, NHS England National Data Engagement Cohort reports, and National Data Guardian publications, were used to inform this summary.

All findings reflect views from diverse members of the public, ranging from general population surveys to in-depth deliberative workshops. The insights highlight the common ground in public expectations for data handling beyond SDEs in the UK.