North East and North Cumbria Secure Data Environment

Targeted engagement – findings

A document by Stand

Date: April 2025

Contents

1 Background

Patient and Public Involvement and Engagement (PPIE) plays a key role in delivering the Secure Data Environment (SDE) programme for the North East and North Cumbria. One of its activities includes targeted work with specific communities across the region.

In 2024, research was conducted to gather local perspectives on the development of an SDE for the North East and North Cumbria and the use of health and care data within it. This study led to the identification of a detailed set of demographic 'persona types (see Table 1 for more detail).'

- **Affluent educated** – People who are well educated and more affluent i.e., those with higher household incomes
- **Cultural collectives** - Ethnic minority communities including established immigrant and the Jewish communities
- **Remote Residents** – People living in larger communities outside major conurbations but without full access to key services
- **Cautious Women** – Women aged 30 – 59 years identified in specific areas of the region and unwilling to share health data/keen to opt out
- **Diverse Deciders** – People on lower incomes with varied needs, who are struggling to make ends meet
- **Starting Outers** – Students, young couples and singles in flats

In August, 2024 a further on-street/in-person surveying was carried out with a larger sample size (in response to a requirement in relation to the S251 application). Comparing this to baseline research from the original benchmarking surveying in January 2024, there is some conflicting insight in relation to some of the persona's (remote residents and cautious women) who initially identified as having more negativity towards data sharing – now appearing to be more supportive. Respondents from Cumbria and Northumberland appear happier about sharing the health record. In contrast, those living in Teesside, Durham and Newcastle were less happy about doing so, with those from Durham and Newcastle also having greater concerns about the risks involved and less trust that their health record would be shared for the described purposes.

To build on these insights, a series of focus groups were held in March and April 2025. The purpose of these focus groups was to 'deep-dive' the views held by these communities, to identify any underlying issues people may have around the concept of the SDE.

Table 1: Target persona types identified for the focus groups

<table>
<tr><th>Remote Residents</th><th>People living in larger communities outside major conurbations but without full access to key services</th></tr>
<tr><td colspan="2">This is a distinct geographical group. An analysis of national opt-out data revealed that Northumberland has the highest opt-out rate (5.16%; 336,500 patients) among all North East and North Cumbria sub-ICBs. Notably, areas around Morpeth, Cramlington, and Hexham exhibit higher national opt-out proportions than other parts of the region.
Given these findings, this population may experience a greater impact from the SDE programme, making them a key target group for engagement and further research.</td></tr>
<tr><th>Cautious Women</th><th>Women aged 30 – 59 years identified in specific areas of the region and unwilling to share health data/keen to opt out</th></tr>
<tr><td colspan="2">A street survey conducted in January 2024 across the North East and North Cumbria revealed that dissatisfaction and distrust regarding sharing personal data in the SDE was highest among individuals aged 35–44.
This age group also expressed heightened concerns about sharing data with charities, universities, pharmaceutical companies, and care agencies. Their primary reservations cantered on data security, particularly the risks of unauthorised access or potential data leaks.
Additionally, women aged 30–59 have been identified as a key demographic likely to be significantly impacted by the SDE programme.</td></tr>
<tr><th>Diverse Deciders</th><th>People on lower incomes with varied needs, who are struggling to make ends meet</th></tr>
<tr><td colspan="2">An analysis of national opt-out rates by Acorn type revealed that diverse young families living in rented terraces and flats (Acorn Group 6.S.56) are less likely to opt out (1.6%) compared to more affluent and prosperous demographics.
Within this group, 8% of adults hold a degree, and the mean gross household income is £27,000. Given the everyday challenges these individuals navigate, it is crucial to assess how the SDE programme will impact them and address their specific needs effectively.</td></tr>
<tr><th>Starting Outers</th><th>Students, young couples and singles in flats</th></tr>
<tr><td colspan="2">Students and individuals sharing multi-occupancy flats have been identified as the most concerned about online data security. However, findings from the Office for National Statistics (2023) suggest a contrasting trend—young adults, particularly those aged 18–24, often do not question or actively worry about data sharing. Having shared personal information throughout their lives, they perceive little impact in disclosing additional data, given how much is already publicly available.
This contradiction highlights the need for deeper exploration of this demographic's attitudes, particularly regarding the use of health data for both research and non-research purposes. Understanding their perspectives will be critical in shaping engagement and communication strategies within the SDE programme.</td></tr>
</table>

2 Methodology and sample

Residents of the North East and North Cumbria were invited to express interest in participating in focus groups about the SDE programme. Recruitment efforts included:

- Targeted social media outreach (Facebook posts and advertising)
- Local Healthwatch organisations
- GP practices
- Voluntary sector organisations and community groups

All residents that expressed interest were asked a series of demographic questions. The responses to which were used to identify participants who fell within the different persona profiles: Remote Residents; Cautious Women; Diverse Deciders; And Starting Outers.

In total, six focus groups were conducted, each lasting 90 minutes, with both daytime and evening sessions held to maximise participation. Through these discussions, we gathered insights from 29 individuals, ensuring a diverse range of perspectives were heard. Participants were incentivised with a £40 Love2Shop voucher for their time and contribution.

Table 2: Focus group schedule

	No. of attendees
Tuesday 25th March; 6-7.30pm	3
Wednesday 26th March; 12.30-2pm	5
Thursday 27th March; 6-7.30pm	7
Tuesday 1st April; 6-7.30pm	3
Friday 4th April; 12.30-2pm	4
Wednesday 9th April; 6-7.30pm	6
Telephone interview	1
Total	**29**

Table 3: Respondent sample by persona type

	No. of attendees
Remote Residents	9
Cautious Women	14
Diverse Deciders	5
Starting Outers	1
Total	**29**

3 Key findings

3.1 Key findings from the focus groups

Initial thoughts and feelings

Opinions on sharing health data varied. In general, people were supportive of anonymised information being included in the SDE. Some participants supported sharing their information when it served a greater good, for example advancing health and care knowledge and services, whilst others caveated their support or required reassurances (e.g. about the anonymisation process).

Respondents have greater reservations about data sharing with pharmaceutical companies, primarily because they are perceived to be profit-driven rather than public-focussed. This distrust extends to organisations outside the NHS such as universities, charities, care agencies, and local authorities.

Digital literacy and generational awareness affect how comfortable people feel with sharing their health data. Older people are more sceptical about using digital technologies, whilst younger people are more comfortable with data tracking and sharing information. It was suggested that people falling within the 35 – 44 age cohort might be more hesitant to share their information due to responsibilities that come with this stage of life.

Consent and control

There is strong support for choice in data sharing, with many considering the ability for people to opt in or out as essential. Further, some respondents felt strongly that people should have the choice of what data to share and with whom it is shared. Concerns were however raised about the statistical validity of the dataset if people opt their data out.

Ensuring patients have the time and space to make informed decisions about data sharing was also considered crucial.

Security and trust

Concerns about data security included potential breaches, misuse, and risks tied to anonymisation. Because data within the SDE holds significant value, people were worried it could become a high-priority target for cyberattacks.

Some people were concerned that even anonymised information could be linked to specific individuals. People were worried that organisations, hackers, or human error could uncover their identities. Questions were also asked as to how useful the data would be after stripping out context and details.

Building trust

Ensuring strong governance, clear rules, and well-defined consequences for misuse of data is essential for maintaining public trust. Participants discussed the importance of clear policies on handling data breaches and having robust security measures and systems to safeguard data. Limiting access to named individuals was discussed as a method to improve accountability.

Participants across all groups felt that building public awareness and understanding of data security and safeguards would help ease concerns about data sharing in the SDE and help build and maintain trust. Trust can be strengthened by ensuring clear, accessible information and providing clarification about how peoples' data has been used.

Transparency is a central theme across the participant feedback. Clear, accessible communication is crucial for building trust. There is a need to tailor communication campaigns and information to different age groups, and use various methods, ensuring information was accessible to all.

Involving people

People highlighted several ways they would feel comfortable contributing more feedback into the development of an SDE programme. To ensure meaningful public participation, there is a strong call for an inclusive and accessible approach to engagement. Public ownership of data is emphasised. Involving young people in discussions about data ethics is seen as valuable.

Differences between persona types

Each of the four persona groups have unique characteristics and perspectives about the use of health and care data. By understanding the key differences between these personas, we can better address their specific needs.

- **Cautious Women** had a heightened concern about data security. To support Cautious Women to share their information in the SDE, the programme needs to offer robust governance and strict adherence to GDPR across all organisations handling health data.
- **Remote Residents** are concerned about data security and the potential for data breaches. For Remote Residents, they need to have greater control of their information. They felt strongly that people should have the control to opt-in or out of sharing their information.
- **Starting Outers,** particularly younger adults, often do not question or actively worry about data sharing. The SDE needs to support patient choice with sharing their data for this persona group. The programme needs to emphasise transparency and education to help this cohort understand the benefits of sharing their data.

- **Diverse Deciders** question whether anonymised data would be useful. They emphasise the need for clear, accessible information and providing clarification about how people's data has been used. The SDE programme needs to ensure it has strong public awareness and education.

4 Findings from the focus groups

4.1 Initial thoughts and feelings

Opinions on sharing health data varied. In general, people were supportive of anonymised information being included in an SDE. Some participants supported sharing their information knowing that it served a greater good.

> *“I would be happy for my data be used in research because it would improve treatments, and it would help the NHS and other services to treat patients.” (Remote Resident)*

Others added caveats to their support or needed reassurances, such as explanations of what is meant by anonymisation as well as information about who will have access. The process of anonymisation reassured people that their identities will be protected whilst still allowing their data to be used.

> *“… you explained what you meant about anonymous health data, I did feel a lot more comfortable. And I would like to think that that's useful because I can see. there are obviously massive benefits to that data” (Cautious woman)*

Some felt comfortable with sharing their health data in the SDE because of its connection to the NHS, which added a layer of trust.

> *"I don't mind the NHS sharing my data but it worries me more about who can get their hands on it outside of the NHS" (Remote Resident)*

While some people support data sharing in principle, they worry about how the information might be used beyond its original intent. Others are more sceptical, expressing distrust in the system and questioning whether anonymisation is truly effective.

Cautious Women had more reservations about sharing their information into the SDE:

> *"Part of me would really like to help, I think it would be really good, it's just the security risks that are holding me back" (Cautious Woman)*

> *"I don't want to be withholding my data, but it's very important to me and it's my life and I just don't want anybody having access to it, I'd want to know how my data was going to be used" (Cautious Woman)*

They were also more likely to say they did not support sharing their data:

> *"I personally don't feel like having this thing where our data can be shared for research. Increases the risk of, you know, in terms of data security." (Cautious Woman)*

> *"I think it's not as simple as do I trust it? Well, I don't trust, I don't trust anything to do with data because I don't think we should. I think we should always be sceptical" (Cautious Woman)*

4.2 Consent and control

4.2.1 Opting-in / out

Respondents felt strongly that people should have the choice of what data to share and with whom it is shared. They felt people need to be able to give informed consent to share their information and choose whether to opt-in or out of sharing information into the SDE.

Respondents wanted clarification over what information will be shared, how that information will look, and why the information is being shared. Knowing this would help people to feel more comfortable and in control.

> *"Having opt-out/in is fundamental to ethical research practices and essential for building and maintaining trust" (Starter Outer)*

Concerns were raised by some about the statistical validity of datasets if people opt their data out of the SDE. It was noted that if too many people exclude their data, it could affect the reliability of research results, and the decision made on that research.

Cautious Women recognised it would be impractical for data controllers to manage people's requests by individual projects or health information. Therefore, there was a need to balance people's choices with the need for comprehensive, high-quality data.

> *"… how on Earth you know, if you asked people to opt in or out of things, I can't. I mean, for a start, can you imagine there'd be billions of them a week?" (Cautious Woman)*

They were also more likely to feel people should have the option to opt-in or out of sharing information, but from the perspective of alleviating concern.

> *"If they could do something specific so you could choose exactly what projects you opt in to so you know exactly what your data is*

> *being used for, I think emotionally that would make me want to help more, I might put the security to the side then" (Cautious Woman)*
>
> *"I think I would be a lot more willing if to engage in the process if I was able to opt out on something that I felt really strongly about. So I think that would definitely change my mind in terms of sharing data in in like a secure data environment." (Cautious Women)*

Remote Residents felt strongly that people should have the ability and control to opt-in or out of sharing their information:

> *"I would want to give my permission, I would like to be notified about what they were using it for so I can make the decision if I want to give up my data" (Remote Resident)*
>
> *"I am really concerned about how anonymous data is getting people's informed consent" (Remote Resident)*

4.2.2 Choice over what data to share

Individuals want control over their data, including the option to consent to different parts of their health records being shared. For example, choosing not to share mental health information while allowing other health information to be used. Some people felt this information was more personal and sensitive. Others were worried about the personal repercussions if mental health information became identifiable. Clear opt-in and opt-out processes are needed to ensure informed consent and transparency, and to increase trust and confidence.

Remote Residents and **Cautious Women** had more apprehension about sharing mental health information in the SDE. They felt there should be the option to opt in / out of different parts of records being shared

> *"There's some things that may be helpful to others and some things that I wouldn't want shared" (Remote Resident)*
>
> *"I would like confidence in how that data is going to be used and have some sort of say in what type of data" (Cautious Woman)*

4.2.3 Clarity over sharing information

In addition to the type of information to be shared, some participants wanted control over who their information is shared with. People did not want their data to be sold.

They wanted to understand how it will be used, and who would benefit from the research.

Many respondents questioned what type of data would be shared in the SDE, with some automatically thinking about the detailed notes taken by GP Practices and other health care services.

> *"What level of detail is it, can they read our entire medical record, all our history, every conversation with doctors, because that would feel a bit of an invasion of privacy" (Cautious Woman)*

Following on from the assumption that medical notes would be shared in the SDE, **Remote Residents** questioned how thoroughly their information could be anonymised to protect their identities.

> *"I'd be worried about slip ups in how anonymous the data will be given that it's coming from multiple sources" (Remote Resident)*

> *"Is it being a properly anonymised at the point of collection? Because once you're past that and you become part of the population as a whole" (Remote Resident)*

4.3 Security and trust

4.3.1 Associated risks of sharing health data

Anonymisation

People were particularly concerned with anonymising data. This included wanting a better understanding of who is responsible, and how the process will work. They also wanted to know what information would be shared, and what the final data would look like. Many people were worried that sensitive information, like GP notes which included personal and identifiable information, may be difficult to fully anonymise.

> *"I'd be interested in finding out who will be doing the anonymisation part, before it goes into the SDE, what kind of company or who actually does it?" (Remote Resident)*

Loss of meaning

People also questioned whether anonymised data would be useful, acknowledging that stripping out identifying details could remove crucial context. This could hinder accurate interpretation of the data, leading to incorrect conclusions or decisions.

> *"How will they cleanse data without losing valuable and relevant information i.e. it has got so small it's not useful" (Remote Resident)*

Identifying people

Some people were concerned that even anonymised information could still be linked to specific individuals, particularly those with rare medical conditions or those in smaller geographic areas. This raised doubts about whether anonymising information truly protects people's privacy.

> *"By the time you get three or four pieces of information, then you've got something that if the wrong person gets their hands on it, they could start to track particular people down". (Remote Resident)*

It was suggested that information be stripped of any data which could be used to identify people by narrowing down fields before it enters the SDE.

> *"Have a database that is pseudonymized and has the patient records in there so they don't know who the patient is, but to a geographical level that is not identifiable." (Remote Resident)*

De-anonymising data

There were fears that organisations or hackers could still uncover people's identities. Additionally, human error, such as incorrectly transposing patient codes, adds another layer of uncertainty. Ensuring identifiable information is completely removed is crucial to maintaining both security and usability, and for building public trust. People also questioned how anonymised information could be reversed to help inform people of its use.

Data security and misuse

There are several concerns about data security, including potential breaches, misuse, and risks tied to anonymisation.

> *"There will be hacks straight away, no two ways about it, this data is worth millions" (Remote Resident)*

Deliberate threats, such as hacking, could lead to sensitive data falling into the wrong hands, while accidental breaches, like users leaving systems open, also pose risks.

With the data in the SDE holding significant value, there was concern that it could become a high-priority target for cyberattacks. People were concerned that information would either not be used for the original intended purposes or be used for reasons beyond its original intended purposes. This concern was mainly directed at organisations outside of the NHS, or organisations with a commercial interest in the data (e.g., pharmaceutical companies, charities, universities).

> *"I would not give me consent in case of misuse including profit making, data is a valuable commodity." (Cautious Woman)*

The NHS and data security

There were mixed opinions as to whether the NHS does enough to ensure data security. Some people had faith that the NHS would protect the information in the SDE, and that the information was secure. However, more people identified how the NHS has already had data hacked, or how they've had personal experience of their information not being kept secure within the NHS.

Remote Responders were more likely to identify examples of when NHS data had not been secure in the past:

> *"The NHS, I don't think they do enough to secure data you hear about quite regularly. [AND] I'm just reading that a total of 897 data breach claims were lodged against the NHS trusts between the financial years of 20/20/21 and 20/22/23 so. It is a bit worrying" (Remote Resident)*

> *"I'm cross matched with another patient, my medical records don't belong to me, they belong to somebody else and I'm trying to sort that out. If they can't get that basic level right, what are they going to do with everybody's data?" (Remote Resident)*

Robust data security

In considering what robust data security would look like, people wanted:

- A secure system, which could not be hacked.
- Controlled access, with restricted access and secure passwords.
- Strong governance, with structures and procedures for data access, and
- Accountability, where people are held to account for misuse.

Overall, distrust in security remains, with questions about how user authorisation is managed, who oversees access, and how the system will maintain data integrity if transitioned to a new provider or operating system. Strengthening security measures, ensuring transparency, and addressing concerns proactively will be key to building trust in the SDE.

> *"Who is getting that information, you know who is collecting that? Who is in the process? What happens if there is a breach?" (Cautious Woman)*

4.3.2 Sharing health data with different organisations

Concerns around data access within the SDE programme largely centre on trust and governance.

Pharmaceutical companies

Pharmaceutical companies are particularly distrusted by participants. They are viewed as profit-driven rather than public health-focused, with scepticism about their motives for accessing the SDE. Many perceive them as valuing data as a commodity. There is also concern they would misuse data for their own benefit.

> *"The idea that we're all going to be floating around in cyberspace to every pharmaceutical company - I don't like the idea of that."*
> *(Cautious Woman)*

Non-NHS organisations

This distrust extends to organisations outside the NHS, with concerns that their governance processes may not be as robust. Participants were uneasy about these organisations handling their data and felt there was an increased risk of security breaches.

> *"I trust the NHS, but concerned about data leaving the NHS - the benefits of data sharing needs to be carefully balanced against the risks of errors and loss of public trust" (Starting Outer)*

There are concerns related to universities, charities, care agencies, and local authorities, especially regarding data security and ethical use. Some respondents believe that senior figures within charities may have links to private companies, raising fears about potential conflicts of interest and whether health data would be used for purposes beyond public benefit. Some worry that universities may not adhere to the same stringent research protocols as NHS organisations, increasing the risk of data breaches. Similarly, concerns about local authorities include fears that they could use insights gained from health data to target individuals unfairly.

> *"I don't think they need that information, I don't think they need that kind of data. Too many charities are money making organisations and I don't think public health is in their best interest, they shouldn't be privy to that kind of information." (Remote Resident)*

4.4 Building trust

4.4.1 Safeguards and governance

Ensuring strong governance, clear rules, and well-defined consequences for misuse is essential for maintaining public trust.

> *"Is there something going to be put in place like a legislation or something that's going to obviously not stop it but going to make people feel a little bit more secure than they do now." (Starter Outer)*

There is a need for clear policies on handling data breaches, including informing affected individuals and reassuring them about anonymity.

Preventative measures, such as secure workplace policies restricting access to personal devices and emails on company equipment, can help reduce risks, as well as provide reassurance.

> *"Clarity around the processes would reassure me." (Starting Outer)*

Organisations such as charities and universities, that are allowed access to data must have strong governance structures in place to protect data and prevent misuse.

Robust security measures and systems are critical to safeguarding data, with features such as antivirus protection, strict password requirements, and automatic system locks when devices are left unattended.

Limiting access to only a small number of named individuals would improve accountability, ensuring those handling data can be held responsible in the event of a breach.

Strengthening safeguards and maintaining open channels for accountability will be key to ensuring data governance meets public expectations.

Cautious Women emphasised the need for robust governance and strict adherence to GDPR across all organisations handling health data. They advocate for clear consequences for misuse or mishandling of information, ensuring accountability in the SDE programme.

To further reinforce transparency and public trust, they also support the establishment of a well-defined complaints process, allowing individuals to report concerns to an independent body. Additionally, advocacy groups could play a vital role in assisting those who may find it difficult to raise complaints independently, ensuring fair representation and protection of public interests.

> *"If somebody feels really uncomfortable about the data being used, how can they make complaints and who will actually deal with that? Who will our independent body be" (Cautious Woman)*

> *"There should be advocacy groups for them to be able to make their complaints, a lot of people aren't capable of doing that" (Cautious Woman)*

4.4.2 Awareness and education

Building awareness and understanding of data security and safeguards is crucial for alleviating concerns and maintaining public trust. Participants across all groups felt that better public awareness and education could help ease concerns about sharing their health data in the SDE. This would mean people fully understood how their data would be anonymised, what was meant by data sharing, and the benefits it can bring.

> *"Might be one of the things that would you know, help a lot of people to give consent. I think if that was understood, it would certainly in my case anyway." (Diverse Decider)*

A lack of awareness can erode trust, and a lack of education on how technology manages personal information can lead to uncertainty and scepticism. Providing clear explanations and accessible education would help individuals make informed decisions and feel more confident about data usage.

Cautious Women were more likely to be advocates ensuring people were informed, aware, and educated about the SDE. They felt people would be more reassured with greater awareness and education. Incorporating areas like technology, safeguards and security, the benefit of research, and what anonymised information looks like:

> *"If people feel informed and reassured then they are more likely to comply and want to use their data to help"*

> *"I think everybody should know what they're going into. You know, you want to know why am I doing this? What's the benefit? All the questions, what's going to be the outcome?"*

> *"… adding on to others that have said about education is that perhaps as the society, we need to understand more" AND "what's the benefit of it and the benefit of it being used for research to benefit people?"*

Trust can be strengthened by ensuring clear, accessible information and providing clarification about how peoples' data has been used. Transparency is essential, with calls for systems that allow individuals to track who has accessed their data and for what purpose.

> *"Get an annual statement of who has been looking at / using your data and what their intention is for that data" (Cautious Woman)*

Additionally, more effort is needed to inform the public, including publishing a clear list of organisations with access to data. Strengthening education and visibility in these areas would enhance understanding and trust in data governance.

4.4.3 Consent and control

Ensuring patients have the time and space to make informed decisions about data sharing is crucial.

> *“People should be able to be giving informed consent, so they should be given information about what the purpose is of the research project.” (Cautious Woman)*

Consent should be given in a non-pressured environment, avoiding urgent situations like A&E where individuals may not have the capacity to properly consider their choices.

Clear opt-in and opt-out processes are essential, allowing patients to control how their data is used across the SDE and within different organisations.

4.5 Different attitudes for different populations

4.5.1 Digital literacy and generational awareness

Digital literacy and generational awareness affect how comfortable people feel with sharing their health data in the SDE.

Older people could be more sceptical about using digital technologies and feel uncomfortable with the constant data tracking that occurs via tools like Alexa, Facebook, and Instagram. The advances in technology could deter some older people from sharing their data.

> *"My mom won’t even have Alexa in her house, and she doesn’t even like to talk in my house because she thinks Alexa is listening to our conversation and everything" (Starter Outer)*

> *“I've got a mother. Who is not tech savvy, she would absolutely not share her data with anyone” (Cautious Woman)*

In contrast younger people are more comfortable with data tracking and sharing information, largely due to their exposure to technology and social media growing up. It has made them less concerned about privacy.

> *"I say to my mum she needs to embrace it like we have, we can't control it" (Starter Outer)*

4.5.2 People aged 35 – 44

When asked why the 35–44 age group might be more hesitant to share their information, respondents pointed to the responsibilities that come with this stage of life. People in this age group often have school-age children, so they think more about consent because it's regularly discussed at schools.

People in this age group often juggle financial responsibilities and worry about identity theft, making them more cautious about sharing personal information.

> *"I guess it's that fear of, you know, when we hear that whatever phone company has had data leaks that that implies, I guess to me financial risk. Risk of my identity being taken over so" (Cautious Woman)*

Finally, it was suggested that people in this age group may be starting to use healthcare services more. And therefore, have more data included in their health records than younger people.

There was also the contrasting assumption that older people may be less concerned about sharing their data as the impact wouldn't affect them.

4.5.3 Supporting different age groups to feel comfortable

The discussions revealed differences in people's awareness, understanding, comfort with technology, and life stage. Awareness and understanding vary across age groups, with younger people often viewing data sharing differently from older generations.

This identifies that people define 'data privacy' in different ways, depending on the generation and comfort levels.

Therefore, there is a need tailor communication campaigns and information to different age groups. Information that is shared needs to be transparent and explains the SDE process clearly, so people can understand.

> *"We need to know that this is exactly what's going to happen, and this is the procedure. It needs to be very clear, although I am happy to share my information for research, I can completely understand these concerns" (Cautious Woman)*

4.6 Transparency and public involvement

Transparency is a central theme across most participants, especially around:

- What data is being collected
- Who is using it
- What it will be used for
- What happens after the research

4.6.1 Communication

Clear, accessible communication is crucial for building trust, with participants calling for better public education and awareness, and more opportunities for individuals to have control over their data. Public involvement in data decisions, through opt-in options and clear disclosure of data usage, is viewed as necessary for ethical data sharing.

> *"I think that's where the issues probably would stem from … a lack of understanding and a lack of knowledge. Which then would very easily lead to being fuelled by nervousness or uncertainty. Which can be addressed through communications and through information." (Remote Resident)*

People felt this communication should use several methods. Some of the methods identified to support communication include:

- Media campaigns
- TV programmes / documentaries
- Engage with specific groups, like community leaders / VCSE
- Through email / newsletters
- By post
- Text message

There was a call to make this information more accessible:

- Clear, simple language, using plain English and avoiding acronyms to ensure everyone can understand.
- Available in different languages and formats - to reach diverse communities.
- Trusted channels – working with GPs, Community leaders, and charities to share information in a familiar environment
- Community engagement - through public meetings, workshops, discussions, and local events.
- Using real-life examples, so people can relate to other experiences.

4.6.2 Involving people

People highlighted several ways they would feel comfortable contributing more feedback into the development of an SDE programme for the North East and North Cumbria, including:

- Public engagement – particularly on new proposals for data use and sharing
- Events run through trusted channels, to cater to individual communities (such as community leaders, and VCSOs)
- Public panels and group discussions
- Surveys, which some people found more accessible

Some people had concerns about citizen juries and similar participation models. They worried that requiring expertise might exclude some people and limit the knowledge and insights that could be shared. Also, the term "citizen jury" was felt to be unwelcoming by some. A key issue questioned was how much influence the public has in decision-making using a citizens jury.

> *"You are pushing certain individuals out and attracting others, which is not fair" (Remote Resident)*

4.6.3 How people can influence

To ensure meaningful public participation, there is a strong call for an inclusive and accessible approach to engagement. Establishing a clear line of contact for individuals to voice their concerns is essential, alongside proper training in GDPR and safeguarding for those involved.

Efforts must be made to avoid hearing from the same voices repeatedly, ensuring a diverse range of perspectives. A regulatory board that is independent from the SDE programme team, including public representatives, is recommended to ensure transparency and accountability.

> *"So they can listen and phrase our concerns in a way that these institutions would listen to, having a regulatory body who holds these companies or the NHS or whoever accountable would be really helpful" (Starting Outer)*

Public ownership of data is emphasised, with everyone having the right to be involved in decision-making.

> *“So it's not just us, it's not us and them us and you we want to do this collaboratively and I think collaboration and working together is a big thing” (Cautious Woman)*

Involving young people in discussions about data ethics is seen as valuable, as they offer fresh perspectives and insights into evolving digital practices.

4.7 Differences between persona types

Each of the four persona groups have unique characteristics and perspectives about the use of health and care data in an SDE. By understanding the key differences between these personas, we can better address their specific needs, work to alleviate concerns, and increase confidence in the programme. This also helps us ensure engagement and communication programmes are targeted towards the needs of these groups.

Cautious Women

This persona had a heightened concern about data security. Particularly, around the risks of unauthorised access or potential data leaks. They expressed distrust in sharing data with charities, universities, pharmaceutical companies, and care agencies. They were generally more unwilling to share health data and were keen for the control to opt-out of sharing some or all their data. They emphasise the need for robust governance and strict adherence to GDPR across all organisations handling health data.

To support Cautious Women to share their information in the SDE, the programme needs to offer robust governance and strict adherence to GDPR. This would address their concerns about data security and unauthorised access. Ensuring data is anonymised and used ethically, with transparency about what this means, would help build trust and encourage them to share their health data.

Remote Residents

Remote residents are concerned about data security and the potential for data breaches. They also question how thoroughly their information can be anonymised to protect their identities. They feel strongly that people should have control to opt-in or out of sharing their information. They are more likely to identify examples of when NHS data had not been secure in the past.

For Remote Residents, they need to have greater control of their information, allowing them to opt-in or out of sharing their data. Concerns this persona has around data breaches may be eased somewhat through having this control, and through the reassurance of data anonymity. In addition, the programme needs to be transparent with clear communication to help build trust in this group.

Starting Outers

Younger adults often do not question or actively worry about data sharing. They are more comfortable with data tracking and sharing information due to their exposure to technology and social media growing up. They support patient choice in data sharing and consider the ability to opt in or out as essential. They emphasise the need for clear policies on handling data breaches and informing affected individuals

The SDE needs to support patient choice with sharing their data for this persona group. Concerns about data security could be alleviated through the provision of policies on how it would handle data breaches and how it would communicate with affected individuals. The programme needs to emphasise transparency and education to help this cohort understand the benefits of sharing their data.

Diverse Deciders

They question whether anonymised data would be useful and whether stripping out identifying details could remove crucial context. They advocate for better public awareness and education to help ease concerns about sharing their health data in the SDE. They emphasise the need for clear, accessible information and providing clarification about how people's data has been used.

The SDE programme needs to ensure it has strong public awareness and education. This would help alleviate concerns Diverse Deciders have about sharing their health information. By providing clear, accessible information and clarification about how people's data has been used, the programme can build trust and confidence. Additionally, the programme needs more clarity on anonymised data, including how it can retain its usefulness and context for data research.