Yorkshire & Humber SECURE DATA ENVIRONMENT

Part of the **NHS Research Secure Data Environment Network**

NHS

Secure Data Environment Comunity Workshop Report

facilitated and reported by Abilities Together CIC

Introduction

Abilities Together CIC is a voluntary, not-for-profit community organisation that has been active since 2015. Its primary mission is to enhance access to green spaces for the local community, promoting both physical and mental well-being. The organisation also provides vital health education and support focused on managing diabetes and other metabolic diseases. Additionally, Abilities Together CIC conducts research aimed at improving diabetes services specifically for the South Asian community in Bradford, addressing the unique health needs of this population and advocating for more effective, tailored healthcare solutions.

Project background

This project was funded through Y&H PPIE work for five community organisations to gather data and public feedback on the use of and creation of Secure Data Environment (SDEs) namely the Yorkshire and Humber SDE. It was necessary to capture the thoughts of the community as stipulated by the funding providers primarily for the purpose of full transparency. Abilities Together CIC were given the opportunity to deliver on this contract. By engaging the public allows them to be fully informed about how their data will be used and reassuring them that there is no risk of unauthorised access. Public trust is essential the aim of this project was to encourage public active support and participation in research by recruiting between 18-30 participants.

Methodology

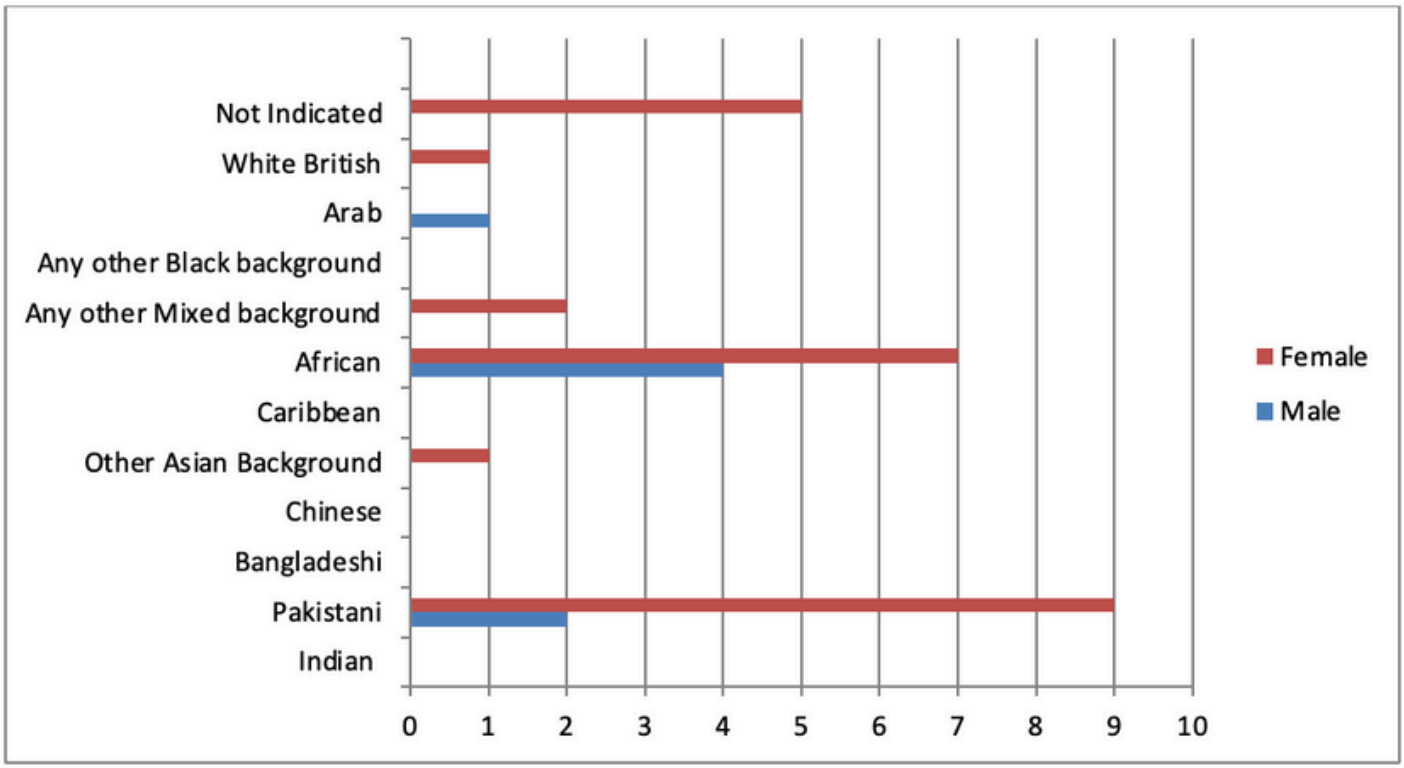
Our aim was to recruit 30 participants from Black and minority ethnic communities. Since Abilities Together CIC primarily works with communities from these backgrounds, we successfully recruited 33 participants. Our participants were services users of the Quaker House in Bradford, these comprised of primarily refugees and English was a barrier as most spoke Arabic. The other groups were made up South Asian men and women. We successfully captured data in from all three groups.

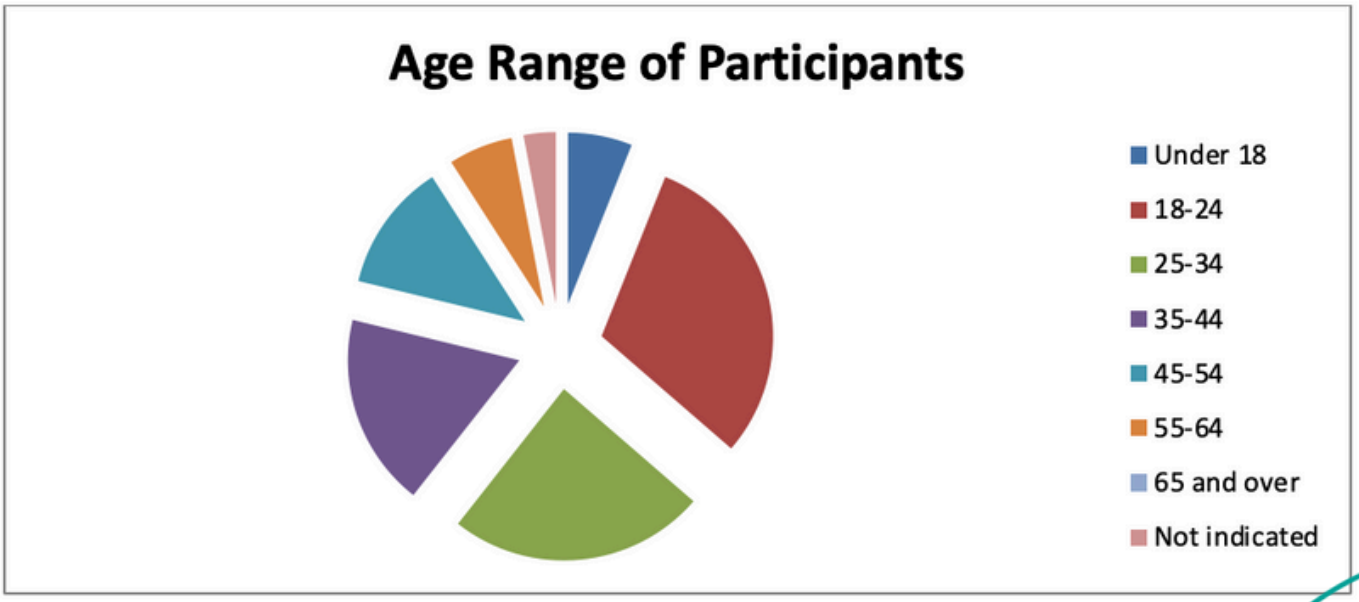
We delivered three focus groups where we introduced the concepts of SDEs, groups were made up of 8 or more participants. Once groups were familiar with what SDEs were we asked questions to the groups and the responses can be found later in the report.

For the two groups of South Asian men and women, these groups were divided into smaller groups of four, to discuss amongst themselves and then document on A3 sheets what they thought of each answer. Since language was a barrier and an Arabic translator was used to interpret the questions from English to Arabic, the refugee group worked better as one group. From the responses provided, we analyzed the answers and identified common themes. All participants were given £20 vouchers for their contribution.

Participants

Below is a graph showing the ethnicity breakdown of participants





Analysis and Discussions

All participants were very vocal during the discussion (see appendix 1 for images of the workshop) various unrelated topics would emerge. It was apparent that the topic did spark interest in overall security of patient data. There was common acceptance and agreement that SDEs are essential for research purposes only. The groups accepted that sharing data for the greater good should be the only reasons for sharing information with legitimate companies and institutes. If patients were to benefit then companies should produce request that are appropriate and useful, otherwise data should be restricted.

Many were fearful of allowing access to organisations, companies and even countries which may have anterior motives, such as requests from Terror groups or regimes which may be damaging to overall public interest. Apart from naming a few countries which were currently heavily mentioned in news outlets, not one group defined what a 'Terror group' was. Furthermore, there was huge distrust for the British government as well as local governments. The NHS, places of education and companies working towards a common benefit were seen as trusted companies who could access the data.

Not one group suggested that SDEs should not exist, these are seen as important facilities. There was an appreciation an almost a sense of acceptance that these SDEs should be created, but through a watchful eye. Such as when asked who should decide who gains access to data, most mentioned that patients themselves, or trusted board of trustees, and from a higher authority made of professionals such as doctors and educational institutes.

There was also yet a sense of fear that how do we actually structure this and will our data to actually remain safe. One group mentioned the death penalty for any breaches of data. This was the level of concern for the data to remain safe and all procedures to remain transparent.

There was a greater level of mistrust of the government having access to this information from the view of the refugees. These individuals were somewhat suspicious of the purpose of the focus group and skeptical why the questioning was necessary. It was important to reassure them that I do not work for the government nor would I share this information with the armed forces or the government.

Most people were very accepting and understanding of the vital role SDEs could potential have for improvement of services namely health services.

See appendix 2 for the breakdown of questions and answers from the groups.

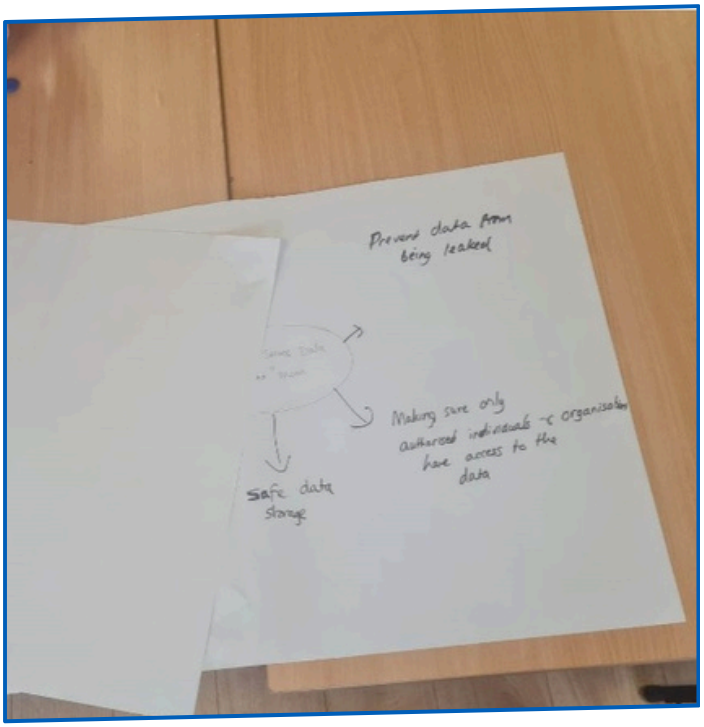
Conclusion

In conclusions it is safe to say that the population group who participated, were engaging and very understanding of the importance and positive work of SDEs. There is still some apprehension of whether information could actually be leaked.

There was a common theme of people trusting the NHS and not having an issue of these groups having access to data. Although a more robust and more convincing solution would be required should third parties require information, all groups were against third parties taking the information. All welcomed secure strategies where the ordinary lay person would be play a role of those responsible for allowing access to data. Many accepted that SDEs would exist and would work in collaboration with education institutes. However, some conspiracy theories did arise and need to be addressed. Therefore, the public needs to be reassured on the safety and in events of breaches occurring as to what would happened to those responsible for the breach of data. The study shows that the public need a deeper reassurance, particularly in relation to current affairs and how many government bodies have been at fault or are the cause of such breaches.

Appendices 1

Images of the focus groups, those participants who agreed, these were groups 1 and 2.



Appendix 2

Groups are broken down as Group 1 and 2 people of South Asian descent, these groups were broken down in to sub-groups of3- 4 people. And Group 3 was of refugees which was a group of 18 people.

Q1. What does secure data environment mean?

Group 1 and 2

1. A database that holds specific information and that is only accessible via secure means of permission. These databases could hold things with generic information. For example 13 boys contracted Asthma, due to poor environment and living conditions, it means a digital library that holds accessible information.
2. Keeping data safe, laws and acts data protection, child protection, control how personal data is used in co-operations. Environment means: Schools, NHS, work place, child social services. Keeping data safe and secure.
3. Keeping data safe, protecting certain characteristics, keeping people safe, keeping data safe, building trust, encryption so only authorized people can have access, confidentiality, personal information for example tissue samples taken due system being 'hacked', data was transferred to non-authorised bodies.
4. Confidentiality, prevent data from being leaked, making sure only authorized individuals and organizations have access to the data, safe data storage, making sure confidential data isn't easily accessible, entrustment.
5. All our data is placed in a secure environment, data is encrypted, password protected data, protected from SPAM, hacking, 2 step authentication, reviewing security of data regularly, data can be shared provided consent is given.

Group 3

Secure data means, personal information, private, safe data, important, sensitive data.

Q2. What benefit do you see in having local health data available for researchers in a secure data environment?

1. Personal information is secure, protected by laws and acts, your information is held by individuals who need it, improves services in health environment, local data allows researchers to gain deeper understanding of community specific health trends and challenges.

2. See what illnesses are most common , which group would be more likely to get ill, find disease, find cure, use it for the future, emergency, see what percentage have different health issues, compare data, see how it affects people.
3. Help with research, potential treatments and effectiveness, analyze conditions, audits, analyze waiting times and effects to reduce waiting times, comparisons – causes and results
4. Data to improve future of healthcare, identify any weaknesses, patterns in healthcare, treatments to see if they are working, early diagnosis of illnesses, early prevention, increases quality of life, stop certain treatments, allocation of resources where required, saves money and lives, identify bigger problems in certain areas: obesity, drug use, crime. More data results in understanding links between current and past studies, increases patients' health and safety, tailor programmes, marketing, training and more research, improve overall economy, improve overall wellbeing and safety, welfare – mental and physical, access to data will be for the only permitted use.
5. Personal information is secure, protected by laws and acts, your information is held by individuals that need it, improves services in health environment, local data allows researchers to gain a deeper understanding of community specific health trends and challenges.

Group 3
Research benefits the community, good secure data is a good thing, gives us valuable insight to what is happening, eg why babies die in hospital, this makes the women happy about knowing the causes of death.

Q3. What are the best ways to tell the public about the secure data environment?

Group1 and 2
1. Public surveys/webinars, campaign/events, media, radio, television, social media, government/NHS, announcements, schools/education announcements, reason made public, access to information, booklets, informative videos, articles, workshops, Q&A sessions, collaborate with influencers.
2. Courses, word of mouth, surveys, social media, blog, articles, newspaper, websites
3. Making people aware of policies, assuring full secure, only accessible by authorized people, advertising in NHA environments i.e. surgeries/hospitals, multiple authentication factors, informing patients about success after using certain data.

4. Reassurance is required provide concise information where it is detailed with consent gained by approved professionals (higher authority). Informing in a way that is comprehended too gain trust and develop rapport with patients, tailored approach and delivering personalized care, not utilizing complex terminology/medical jargon but with words of simplicity. Every group is different, ensure needs are met. Communication: Verbal and non-verbal, behaviour as well as active listening this allows groups to feel comfortable.
5. Leaflets/pamphlets, advertisements, social media, community blogs/forums, ward of mouth community get together/group discussion, public website, press releases and media coverage, influencer partnership.

Group 3
Through social media, Facebook, television adverts at the GP practice.

Q4. What makes you trust sharing your data with other people or companies for research?

Group 1 and 2
1.Having the reassurance that the information will be kept safe and respect people's privacy, keeping it anonymous and not exposing personal information. Research for drugs which help rare diseases people have for better quality of life. Transparency, reputation, compliance with regulations, security measures, consent by individuals.
2.As long as it's used for the purpose its collected for, giving permission for it to be used, allows the research to be conducted, knowing what it'll be used for, reputation of the company.
3.Fully confidential, assurance that personal info i.e. names address not being used, assurance of safety from leakage of data, credibility of the NHS/companies, verified individuals/companies only authorized, knowing that the research will help other people or create cures for illnesses
Understanding purpose of research and reputable companies more inclined to tell.
Anonymised data, if this is made known. Information isn't available to ensure it's believable and regulated this relates to fraudulent activity, reviews of previous candidates to help build an outlook on the company, a positive experience.
2. Reviews, positive feedback, positive changes in the environment.

Group 3
If these are trusted organizations such as NHS, these organizations must be legitimate group

Q5. If companies want to use data, would that be okay?

Group 1 and 2

1. Depends what the purpose is how would data being used be beneficial for the public? It would be okay as long as they adhere to ethical guidelines. Only if the safety and security of the data is put in place. Companies can conduct valuable research while respecting individual's privacy and data rights.
2. Yes it's okay to use data, reason it's collected for, being given permission to use it, should be used for the reason it is collected, sharing to third party without permission is not okay, data shall not be exploited, it is not okay to use data, unless it is used for the purpose it is collected, allows comparisons, upholding laws of data protection Act 2018, general data protection regulations 2016.
3. Is it purely for research? Is it secure? Still don't trust fully.
4. Consent to be given for approval, dependent on purpose if research, if more beneficial more inclined to tell.
5. Helping to improve services, not okay when selling data to third parties, no personal data should be shared this includes name, address and date of birth. Information that should be shared is gender, age, area where you live.

Group 3

Yes, but must be trusted. Will they keep our data safe? Will they use our data wrong? We need to be aware of who is sharing our data, is it on social media, will they sell it? Those with safe infrastructure should use our data.

Q6. Are there any groups or departments that you think should not use the secure data environment? Why?

Group 1 and 2

1.Governments eg Israel, China, fascists, protecting data is crucial for maintaining trust, big Pharma, anyone who uses the data for unbeneficial purposes or uses it against the vulnerable people or mankind for example they could do terrorist attacks.
2.Terrorist, Israelis, Rishi Sunak, government, radical groups, EDL, hackers, black market / dark Web
3.Government e.g. Israel and political parties, foreign governments, commercial use, terrorist organisations.

4.Insurance companies, marketing companies, psychological research groups. Provide transparent data about a cause that can be provided to population further benefit. Inland Revenue and tax, media, councils /local authorities, police – crime prevention, shops selling products.
5. Groups or departments that don't work around the specific data, terrorist organizations, scammers, third parties.

Group 3
We should know the company who is using our data. Are they teachers? Hospitals? We need to know who used our data and how it can be used. Community groups should not have access to the data, only helpful companies. The government should not have our data.

Q7. What kind of requests should not be supported by SDE?

Group 1 and 2
1.Data based on specific demographics, unauthorized access, sensitive information sharing, insecure transmission, illegal activities, independent researchers who do not have a body of people to be answerable, data manipulation, excessive data collection, non-compliance with data retention.
2.Promotional, commercial use, wrong use of data, discrimination purpose, hate crimes.
3.Commercial, name and address requests, religion.
4.Financial data, card details, unknown callers, strangers knocking on the door, exact purpose needs to be known, is it beneficial, relevant to you or applicable, target audience, request causing distress to the community, controversial results, will it harm anyone, discriminatory against someone.
5. Name, address request, nationality for terrorists, religion

Group 3
Request from legitimate organisations only, the army can't make requests, the Government can in some cases some participants felt this because they felt in some cases the Government can help, while others did not wish for the Government to make requests. The participants felt even if the Army wanted data and it was for a good reason, even then requests should be rejected. Most people in the group did not trust the army.

Q8. Who should decide which researchers or organizations can access patient information through the secure data environment?

Group 1 and 2

1. The individual themselves. Responsible people e.g. people with disabilities and mental illnesses cannot make decisions by themselves. Ensure that access is given only to trusted groups who meet the necessary legal and ethical standards.
2. Power of attorney, parents of minor, the person themselves, next kin/carer, having mental capacity, lawyers, governors, patient group/committee, doctors sending it to each other to get a better/second opinion on it.
3. Patients, parents/guardian/next of kin, power of attorney holders, verified panel of people, community – family and trusted people.
4. Procedure is it an approved body? Obtain consent from participants or carers if under 16 years.
5. Yes if opted in for information to be shared, no if opted out, under 18 parents, over 18 years, schools, social carers, health services.

Group 3

Partners, board of trustees made up of patients.

Q9. What kind of work transparency or accountability measures would increase your trust in the Yorkshire and Humber SDE process?

Group 1 and 2

1. Increase the trust in Bradford and Humber SDE process. Complete transparency. Organisations such as OFSTED, better vetting ombudsmen DBS, charity.
2. Death penalty, sanctions, reputation, age of organization/when it is was established. How many people have worked with the organization?
3. Informed about where and how my data is used, who has access of my data, being informed about the results
4. Reputation, trust, structure of company, complaints procedure, doing your own research, performance, registered
1. When sharing information to be clear of what's going to be shared and to whom, such as third parties.

Group 3

We need to be satisfied with the companies' history and background.

Q10. What is the best way to organise and opt-out?

Group 1 and 2

1. GPs, schools, doctors, text messages, online, websites, no time restrictions. Or do they get rid of if after they used it. Can opt-out mean that you can rejoin may change your mind on the decision you made.
2. Text messages, email, word of mouth, letter, online forms, polls, in person, come to my house, talk to my dad, talk to my mum.
3. Email/text, national consent project, through GP
4. Cooling off period, opt-out methods who to contact, letter, text, phone, email, limitation period, scan barcode, clearly communicated.
5. Confirmation has to be made before giving out any information, reading terms and conditions, don't tick boxes to share information to third parties, clear communication which is to be easy to understand, multiple channels in ways of opting out such as emails.

Group 3

To send via email, messaging or letter. We need to take account of the fact that some people with no have access to the internet or other technology.

Q11. What information should we share about the opt-out process?

Group 1 and 2

1.No answer provided.
2.Breach, what/how/why, knowing that your data won't be shared when opted-out, being aware that we can opt-out.
3.Be aware about an opt out option being available, reassurance that once opted out data will not be used, inform me about processes to opt out, how/when/where to opt out.
4.Time frame to opt out, the process, what data is kept and what is destroyed, legalities of data, information that is going to be used, where it's going to be used, how it will be used, when it will be. Informed rights.
5. How information should be shared and to who, if you opt out? Where does information stay? Confirmation should be made when requesting to opt out and when it has been done. How information can be retrieved if needed, different ways to opt out via email, text.

Group 3

Explain what it means to actually opt out, why, how and when and for how long. Is it permanent?