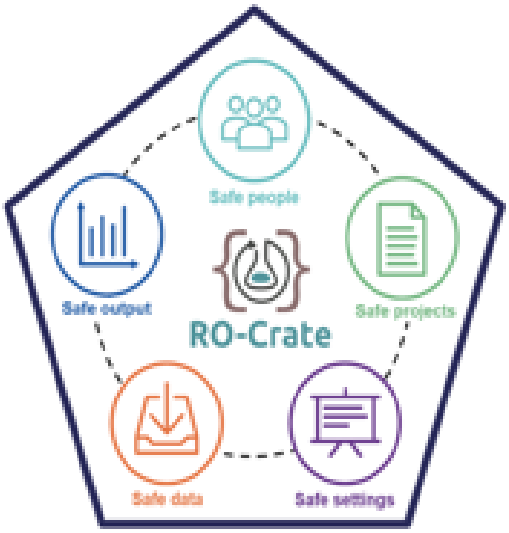
alterline

TREFX Project

Public Consultation Online Focus Groups Report – Phase 2



TRE-FX

DELIVERING A FEDERATED NETWORK OF TRES TO ENABLE SAFE ANALYTICS

October 2023

Compiled by:

Damian Miller,
Research Director
Alterline

DARE UK

Swansea University Prifysgol Abertawe

University of Dundee

MANCHESTER 1824

NHS University Hospitals Birmingham NHS Foundation Trust

University of Liverpool

The University of Nottingham

PIONEER Health Data Research Hub

HDRUK Health Data Research UK

TREFX Online Focus Groups Report

INTRODUCTION

This report represents the full findings from a second series of online focus groups which were conducted to support the TREFX project in engaging members of the public. The research was undertaken by Alterline a third-party research agency that specialise in Academic and University research. Alterline have worked with the University of Nottingham previously on a TRE4C project as well as running the previous phase 1 focus groups in July 2023

The focus groups were conducted through October 2023 and the findings compiled, analysed and brought together here to highlight the insights that have been surfaced from the research.

METHODOLOGY

To capture the thoughts, feelings and experiences of the members of public, Alterline conducted three online focus groups consisting of eight people per group. Participants were citizens of the UK and were a representative mix of ages, genders, backgrounds, education levels and country they live in. An overview of the participants can be found in the appendix at the back of this document.

Each group was taken through the same discussion guide and were moderated by one of Alterline's expert researchers. The discussion guide was created by Alterline and agreed with key stakeholders from the TREFX project group. The guide covered the key areas of understanding and response to the RO Crate explanation and in-depth discussion about two of the Five Safes, Safe People and Safe Projects

These discussions allowed Alterline to explore how the TREFX concept would be greeted by the public, how it might be perceived and what questions or concerns people had about a project of this potential scale. The discussions allowed Alterline to capture the voice of the citizenry in their own words and allow conversations to develop amongst participants and understand the strength of feeling and to what extent there are any universal or divisive elements.

EXECUTIVE SUMMARY

In the context of enhancing public health and fostering research advancements, the concept of safe people and safe projects takes centre stage. This executive summary delves into the perspectives of members of the public concerning the attributes and concerns related to these vital components within the landscape of health data research & Federated Analytics. The discussions are based on a series of insightful comments from a diverse group, ranging from concerns about data misuse to the necessity for stringent regulations and oversight.

Safe People:

The designation of a person or entity as 'safe' in the context of health data research implies a level of trustworthiness, ethics, and reliability in handling sensitive health data. The opinions reflected a cautious approach, emphasising the need for careful vetting and accreditation processes to ensure that individuals or organisations accessing health data possess a track record of responsible data usage.

Attributes associated with safe people include:

- Reputation and Track Record: A safe person or organisation should possess a credible history of handling health data responsibly, substantiated by successful projects and positive references from past endeavours.
- Ethical Orientation: Trustworthy entities prioritise public health benefits over profit, demonstrating a commitment to using health data for improving healthcare and the well-being of individuals.
- Transparency and Accountability: Clarity in the purpose of accessing data and a demonstrated commitment to maintaining data security and privacy are essential features of a safe person or organisation.
- Expertise and Training: Individuals accessing health data should undergo appropriate training to comprehend the sensitive nature of the data and adhere to professional and ethical standards.

EXECUTIVE SUMMARY CONTINUED

Safe Projects:

Safe projects encompass research initiatives that utilise health data to generate insights, drive advancements, and contribute to the improvement of public health. The discussions highlighted a crucial distinction between granting access to data and the utilisation of the data's outcomes. Participants advocated for robust privacy settings and emphasised that data access must be aligned with the intended purpose to mitigate any accidental misuse.

Key characteristics of safe projects include:

- Purposeful Data Utilisation: Safe projects focus on specific research objectives, ensuring that data access aligns with the intended research purpose and reduces the risk of unintended consequences.

- Privacy Controls and Settings: Implementing stringent privacy controls ensures that data is utilised only for the intended research objectives and prevents unauthorised access or misuse.

- Collaborative Governance: Projects conducted in collaboration with trusted entities, such as the NHS, academic institutions and established research organisations, bolster confidence in the project's integrity and responsible data handling.

- Public Health-Centric Outcomes: Emphasising the public health benefits resulting from the research outcomes instils trust in the project's intent and encourages responsible use of health data for the greater good.

In conclusion, establishing a culture of safe people and safe projects in the mind of the public is critical in health data research and Federated Analytics. A robust framework that includes careful vetting, stringent privacy controls, and ethical considerations will ensure that people believe that health data is being leveraged responsibly, ultimately fostering advancements in healthcare and benefiting society at large.

HEADLINE FINDINGS

1. Privacy Concerns are Paramount:
   The public is highly concerned about privacy and anonymity in data research projects. Ensuring the anonymity of individuals and safeguarding sensitive data are critical aspects that need careful consideration in any research involving data collection.

2. Data Security and Trust are Essential:
   There's a pervasive worry about data security and potential misuse. Many individuals are sceptical about how their data is handled and question the ability of authorities or organisations to secure extensive data sets, based on past experiences.

3. Transparency and Informed Use of Data are Demanded:
   People seek transparency in how their data will be used and what the intended outcomes of the research are. They emphasise the need for clear communication about how gathered data will benefit society and ensure that data usage is aligned with the disclosed purposes.

4. Utilisation of Data for Societal Benefit is Recognised:
   While concerns exist, individuals acknowledge the potential benefits of using data to predict trends and tailor services. They recognise the value in using data for targeted improvements in various sectors like mental health services, education, and community planning.

5. Control and Accessibility of Data are Key Considerations:
   The public is concerned about who can access and use the data. Striking a balance between data accessibility and stringent controls is crucial to ensure that data is used for legitimate purposes and prevent misuse.

6. Ethical Considerations and Informed Consent are Emphasised:
   Ethical concerns, especially regarding minors, are prevalent. Individuals stress the importance of obtaining informed consent before collecting data, particularly from young individuals.

HEADLINE FINDINGS

7. Data Granularity and De-Personalisation Must Be Handled Carefully:
   Concerns regarding data granularity and de-personalisation are raised. Individuals worry about the potential for re-identifying individuals as data becomes more detailed and emphasise the need for effective de-personalisation techniques.

8. Trust in Safe People and Projects is Essential:
   The public places a significant emphasis on trust in both the individuals involved in research (safe people) and the research projects themselves (safe projects). Trustworthy and responsible conduct, along with robust security measures, are seen as vital aspects.

These key learnings and findings reflect a need for greater transparency, robust security measures, ethical considerations, and responsible data use. Understanding and addressing these concerns are vital for enhancing public trust and ensuring the success and ethical conduct of data research projects.

The story behind the findings

WHAT ARE THE ATTRIBUTES OF A 'SAFE PERSON/ORGANISATION'?

This initial very open question about safe people was the most difficult question for members of the public to answer. It is very direct and causes participants to stop and think in a way that they have not previously about this project. They do not see themselves as experts who would or should necessarily know what Safe People should be. They openly state that they will have to rely on the institutions that own and manage the project to be able to make those decisions with their best interests in mind. Something that divides opinion at present because they are not fully clear about who would be 'in charge' of a system like this when it is fully operational.

> *Having responsible and ethical individuals involved in the research is fundamental for ensuring data safety.*

With some prompting, participants were able to articulate six key entities they associated with Safe People

1.NHS (National Health Service):
Participants generally expressed trust in the NHS as a safe organisation to handle health-related data, given its role in healthcare and public service.

2. Reputable Universities and Academic Institutions:
Participants considered universities and academic research institutions as safe entities to access and utilise data, provided they have a credible track record and follow ethical guidelines.

3. Trusted Medical Professionals:
Participants mentioned that medical professionals, especially those working within the NHS or reputable medical institutions, could be seen as safe individuals for data access, given their expertise and ethical standards.

4.Individuals with Strong Ethics and Training:
Participants indicated that individuals with strong ethical standards, proper training, and relevant expertise in handling data responsibly could be considered safe for data access.

5. Entities with Credible Reputation and Success Record:
Participants highlighted that entities with a credible reputation, successful past projects, and a positive track record could be deemed safe for data access and utilisation.

6. Companies with a Public Health Focus:
Participants acknowledged that certain companies, particularly those focused on public health benefits rather than solely profit, might be trustworthy for data access in research and healthcare.

Alongside these identified entities there were also some key themes that emerged as important elements associated with the idea of Safe People

Theme 1: Establishing Trustworthy Entities
The National Health Service (NHS)

The NHS emerged as a key entity perceived by participants as safe for handling health-related data. Trust in the NHS stems from its fundamental role in providing healthcare services to the public. Participants viewed the NHS as an organisation with a long-standing commitment to the well-being of individuals. Its status as a public institution dedicated to healthcare further instilled confidence in participants regarding the responsible handling of health-related data.

> *"think, for me, any medical professional, or people that work in companies like Pfizer that want to do some sort of research, I think, for me, people like that*

Theme 2: Ethical Considerations in Data Utilisation
Reputable Universities and Academic Institutions

Participants acknowledged reputable universities and academic institutions as safe entities for data access, provided they follow strict ethical guidelines. These institutions, recognised for their commitment to academic integrity and ethical research conduct, were seen as bastions of responsible data usage. The emphasis on ethical guidelines ensures that data access and utilisation align with principles that prioritise the greater good and adhere to established norms of research ethics.

> *"Trusted researchers and their responsible conduct play a key role in maintaining the safety of data and privacy*

Theme 3: Collaborative and Transparent Partnerships
Collaborative Projects Involving Multiple Safe Entities

Collaborative projects involving both public entities like the NHS and reputable private organisations or academic institutions were viewed favourably. This collaborative approach was seen as a means to strike a balance between public health benefits and data security. Transparency in these collaborations was highlighted, with participants emphasising the need for clear disclosure regarding the involvement of different parties. Such transparency fosters trust and ensures that the collaborative effort is conducted with integrity and accountability.

> *"We need stringent checks and measures in place to prevent unauthorised access and protect anonymity*

Theme 4: Privacy and Data Control
Concerns About Data Usage and Privacy

Participants expressed apprehensions about potential misuse or exploitation of personal data, particularly by external companies or malicious entities. Privacy concerns were paramount, with participants highlighting the need for transparent practices in data usage. They stressed the importance of knowing how data is used and who has access to it. The participants sought a sense of control over their own data, aiming to ensure that their sensitive information is handled responsibly and in a manner aligned with their expectations of privacy.

> *I would want to know what my data has been used for. You know, it's not just being gathered for everyone, but for a specific purpose*

Theme 5: Defining Safe Individuals and Organisations
Individuals with Strong Ethics and Training

The importance of individuals with strong ethical standards, appropriate training, and relevant expertise in handling data responsibly was underscored. Participants considered these attributes essential in designating individuals as "safe" for data access. Ethical considerations were seen as a fundamental criterion for identifying trustworthy individuals within organisations, ensuring that data usage remains ethical, lawful, and aligned with societal norms.

> *Part of the attributes of a safe person might be that they've been trained and understand the nature of the data and these types of things*

Theme 6: Ensuring Ethical Data Utilisation
Companies with a Public Health Focus

Participants acknowledged the significance of companies with a public health focus, as distinct from profit-driven entities, as potentially safe for data access in research and healthcare. The emphasis was on aligning data utilisation with public health benefits rather than purely financial gains. This highlighted the participants' emphasis on ethical motives and the societal welfare aspect when considering organisations for data access and utilisation.

> *I would feel safer if it's coming from the university and not a profit-making company based somewhere else, for the betterment of public health versus a commercial gain*

Theme 7: Balancing Access and Security
Access to Data and Results

Participants differentiated between providing access to raw data and permitting access only to the results or findings derived from the data. Some participants were more comfortable with granting access to results rather than raw data. This underscores the delicate balance between enabling data access for research purposes while ensuring data security and minimising risks associated with exposing sensitive information.

> *It's more a case of having access to the data that could be misused, because it's always the misuse of the data that's the concern*

THOUGHTS ABOUT WHAT WOULD MAKE A PERSON/ORGANISATION UNSAFE

Participants did not explicitly identify specific individuals or organisations as "unsafe" for accessing and handling sensitive data. However, they expressed concerns about certain scenarios and criteria that might raise caution. Here are the areas of concern related to potential lack of safety:

Theme 1. Concerns About Private Companies and Financial Interests:
Participants were cautious about private companies, particularly those driven by profit motives, potentially accessing data for financial gain or insurance purposes, raising concerns about the possibility of misuse.

> *I would say the sponsor would need to sign some sort of agreement that they have done some kind of assessment or background checks on the people they're giving access to*

Theme 2. Lack of Transparency and Disclosure:
Participants voiced concerns about the lack of transparency regarding third parties or contractors involved in studies or projects, highlighting the importance of disclosure and clear identification of involved entities to maintain transparency and trust.

> *signing disclosure agreements, and having clear set out consequences if the data is breached in any way*

Theme 3. Need for Clear Purpose and Ownership:
Participants emphasised the necessity of a clear purpose and ownership, expressing discomfort if a project involved a company from a distant location without a strong affiliation or partnership with a trusted institution.

"I would say the sponsor would need to sign some sort of agreement that they have done some kind of assessment or background checks on the people they're giving access to

Theme 4. Potential for Unethical Use:
There were worries about how large datasets contain unexpected information and the possibility of unintended uses or unethical purposes, indicating a need for careful handling and ethical considerations in data usage.

"I think one of the things we're trying to avoid with the safe people is that you do just say, Well, anyone who works for this company X can do it

Theme 5. Generalised Concerns about Data Privacy:
Participants expressed general concerns about data privacy, especially in the context of modern technology (e.g., smartphones, wearables), underscoring potential risks associated with data collection and privacy breaches.

"I would want to know what my data has been used for. You know, it's not just being gathered for everyone, but for a specific purpose

In depth discussion about Safe People

WHAT ARE THE ATTRIBUTES OF A 'SAFE PROJECT'?

When faced with the potential project scenarios, participants were much more comfortable and engaged with discussing Safe Projects without prompting. In general participants thought the initial ideas of supporting mental health and building a new school were worthy projects. However, there were concerns about how much data was being requested and how widespread that scope felt to them. The feelings expressed were very much about how do you balance the needs to solve complex problems and the desire not to have 'too much' data available in the process. Questions were asked about how granular could the data splits get to and, despite understanding that individuals should not be identified, there was a certain scepticism about how that would work practically.

> *"Implementing strong security measures is crucial for making a research project safe and reliable*

Theme 1. Anonymity and Privacy

One of the foremost concerns in safe research projects is ensuring the anonymity of individuals and safeguarding sensitive data. It is seen as essential to address potential identification risks, especially in smaller groups or specific circumstances, by implementing stringent checks and measures to prevent unauthorised access to personal information.

1.1 Ensuring Anonymity

Anonymity is a cornerstone of safe projects for people. Protecting the identities of individuals within datasets is paramount to prevent potential harm or discrimination. Utilising advanced anonymisation techniques, such as data de-identification and aggregation, would ensure that people feel the project is safe.

1.2 Safeguarding Sensitive Data

Beyond anonymity, safeguarding sensitive data is equally critical. Encryption, access controls, and secure storage are seen as imperative to protect data from unauthorised access, ensuring that only authorised personnel can handle and process it.

> *"Ensuring the anonymity of individuals is crucial in any data research project.*

> *"We need stringent checks and measures in place to prevent unauthorised access and protect anonymity.*

Theme 2. Data Security and Misuse

Safe projects should prioritise robust data security measures to mitigate worries about potential data misuse, security breaches, or unauthorised access to sensitive information. These projects inspire public confidence by ensuring data integrity and safeguarding against unauthorised usage.

2.1 Advanced Security Protocols

Implementing state-of-the-art security protocols is seen as fundamental to data security. Encryption at rest and in transit, multi-factor authentication, and regular security audits were mentioned as components of a secure data environment.

2.2 Mitigating Misuse

To counter potential misuse, comprehensive monitoring systems should be employed to track data usage. Any suspicious activity can be flagged and investigated promptly, preventing unauthorised use or potential breaches.

> *I worry about potential security breaches and unauthorised access to sensitive information*

> *Given past issues with databases, I am sceptical about the government's ability to handle such extensive data securely*

Theme 3. Purpose and Use of Data

Transparent communication regarding the purpose and expected outcomes of the research is seen as a hallmark of safe projects. Addressing public concerns by emphasising the potential benefits of the research to society and providing clarity on how the gathered data will be used is essential for garnering public trust.

3.1 Clarity in Research Objectives

Clearly defining the research objectives and how the data will contribute to achieving these objectives is crucial. This clarity reassures the public about the purposefulness of data collection and usage.

3.2 Demonstrating Societal Benefits

Emphasising the societal benefits resulting from the research instils confidence. Data should be utilised to drive positive change, whether in public policy, healthcare, or other critical areas, ensuring the data serves a meaningful purpose.

> *We need clarity on how the gathered data will be used and what benefits it will bring to society*

> *Questioning the purpose and expected outcomes of the research is essential to ensure its relevance*

Theme 4. Predictive and Targeted Services

Members of the public acknowledge the potential benefits of using data to predict trends and tailor support services to specific areas or demographics. By leveraging data analysis, these projects enhance services and optimise resource allocation, ultimately benefiting society.

4.1 Enhancing Service Delivery

Utilising data to predict trends in various domains, such as healthcare or education, was seen as a way to optimised services. Tailoring services to meet specific needs and demands within communities is understood as an essential outcome of such projects.

4.2 Resource Optimisation

Data-driven insights to enable efficient allocation of resource, by understanding specific demographics and their requirements, was seen as a way to allocate resources where they are most needed, ensuring a higher level of effectiveness and impact.

"Data can help predict trends and tailor support services to specific areas or demographics"

"We should discuss the possibility of identifying trends in mental health conditions and enhancing service delivery through data analysis"

Theme 5. Accessibility and Control of Data

Addressing concerns about who can access and utilise the data was discussed as critical in safe projects. Implementing stringent controls and accreditations to limit access and prevent misuse of sensitive information was seen as a way to ensure responsible data usage.

5.1 Controlled Data Access

Establishing strict controls on data access, specifying who can access certain types of data and for what purposes, was seen as a way to help prevent unauthorised usage and misuse. Ensuring that only authorised individuals can access the data.

5.2 Stringent Accreditation Procedures

Implementing stringent accreditation processes for individuals and organisations seeking access to sensitive data is believed to be critical to limit access only to those with a legitimate need and the expertise to handle the data responsibly.

"Addressing concerns about who can access and utilise the data is critical for privacy and security"

"We need stringent controls and accreditations to limit access and prevent misuse of sensitive information"

Theme 6. Data Granularity and De-Personalisation
Safe projects should carefully consider data granularity and de-personalisation to minimise the risk of identifying individuals as data becomes more granular. Clear guidelines on data granularity would need to be established to prevent compromises in anonymity.

6.1 Effective De-Personalisation
Utilising effective de-personalisation techniques is seen as essential when handling granular data. Concerns about anonymity and avoiding the identification of individuals were expressed by the majority of participants

6.2 Clear Guidelines
The need to establishing clear guidelines on how data should be de-personalised, particularly when dealing with different data sets and varying sizes of data, would help to give confidence and minimising risks associated with detailed and granular data.

“

I'm concerned about the potential for re-identifying individuals as data becomes more granular

“

How data de-personalisation works, especially concerning different data sets and varying sizes of data, needs more clarification

Theme 7. Ethical Considerations and Consent
Upholding ethical considerations and obtaining informed consent, especially for minors, is seen as a fundamental aspect of safe projects. These projects should prioritise ethical data collection and usage, respecting individuals' rights and privacy.

7.1 Informed Consent
Ensuring informed consent from individuals or their legal guardians, particularly in cases involving minors or vulnerable people, was a key ethical consideration expressed. Ensuring that individuals are aware of how their data will be used and can make informed decisions about its usage.

7.2 Ethical Data Collection
Adhering to ethical standards in data collection is paramount. Respect for privacy, ensuring minimal harm, and transparent communication about data usage were seen as foundational principles for safe projects, while promoting the advancement of knowledge and societal progress.

“

I have ethical concerns regarding data collection, especially for children, and the need for informed consent

CONCLUSION

The evolving landscape of health data research presents a dual imperative: to harness the immense potential of data-driven insights for public good and to safeguard against potential misuse. The insights shared in these discussions shed light on the critical notion of safe people and safe projects, highlighting the multifaceted attributes and considerations essential for the responsible utilisation of health data to satisfy members of the public.

Safety in this context is an amalgamation of trust, ethical orientation, transparency, and accountability. Safe people and organisations should possess a commendable track record, an ethical approach that prioritises public health benefits, and a commitment to transparency regarding data usage. Expertise and training play pivotal roles in ensuring that those accessing health data comprehend its sensitive nature and adhere to stringent ethical guidelines.

Similarly, safe projects encompass not only purposeful utilisation of data for specific research objectives but also a comprehensive framework that emphasises privacy controls, collaborative governance, and outcomes focussed on public health benefits. Privacy controls mitigate risks associated with unintended data usage, ensuring that data access aligns with the intended research objectives. Collaborative governance, involving trusted entities, instils confidence in the project's integrity and responsible data handling.

In navigating the delicate balance between data utilisation and data protection, establishing a culture of responsibility and oversight is imperative. Implementing robust frameworks for vetting, oversight, and stringent privacy settings is essential to mitigate the risk of misuse in the eyes of the public. Ultimately, the public sees responsible use of health data, facilitated by safe people and safe projects, propels research advancements, informs policy decisions, and enhances the overall well-being of society.

The insights shared within this discussion serve as a guidepost for stakeholders in the health data research sphere, urging them to prioritise ethical conduct, transparency, and the greater public good. By fostering a culture of safety within health data research, in the mind of the public we can unlock the transformative potential of data while upholding privacy, security, and the principles of responsible research for the benefit of individuals and society as a whole.

Appendix

RESPONSE TO THE RO CRATE EXPLANATION

In general, participants were able to follow the postal analogy example fairly well. It wasn't completely perfect as the fulfilment element didn't quite resonate, but people understood what we were trying to convey. The example was definitely an aid to participants feeling they had a greater understanding of Federated Analytics than they did with just the pre-read materials alone.

The discussions encompassed several critical themes revolving around the RO-Crate process, particularly focusing on the validation of individuals and projects for data access. However, a number of familiar themes also emerge as part of the conversations

Theme 1. Access Control and Validation: The conversations underscored the importance of stringent access controls and validation procedures. Participants expressed the necessity of pre-checks to ensure that individuals requesting data access are valid and have a legitimate reason for access. The need to ascertain if they are the right individuals for the requested data was acknowledged as a key positive in the example

> *"It feels like that adds a level of security to the process that you can't even get in there if you aren't already on this approved list*

Theme 2. Security and Privacy: Concerns about security and privacy are prevalent throughout the discussions. Participants highlight the need to prevent unauthorised access and emphasise the importance of safeguarding sensitive data. Anonymisation of data and preventing data extraction from the system are seen as crucial security measures. Participants felt that there were still details missing from the example that would aid them to build trust in the system

> *"Like, when you categorise, like the correct labels that you put on things, and the correct descriptions? If that's not fool proof at the beginning, does that mess it up a bit?"*

Theme 3. Responsibility and Oversight: The dialogue delves into questions of responsibility and oversight. Participants raise queries regarding who is responsible for the checks and the overall safety of the process. They express a desire for an independent body to manage and oversee the validation process, aiming to ensure unbiased and reliable checks.

> *"There's an element of concern for me about where's the independence coming in? And who's checking the checkers?"*

> *"Who are they going to trust? There's been too many breaches through in all kinds of these businesses*

Appendix

RESPONSE TO THE RO CRATE EXPLANATION

Theme 4. Potential Biases and Independence: The discussions touch on concerns about potential biases arising from a single governing body performing all the checks. Participants suggest the need for independent oversight and express worries about unchecked authority, emphasising the importance of unbiased governance.

> *If it is one authority that's doing all of these checks, there needs to be some form of governance of them as an organisation to have the ability to be able to do that*

Theme 5. Collaboration and Duplications: The dialogue also addresses collaboration possibilities and the potential to remove duplications in research requests. Participants suggest mechanisms to identify similar research requests and propose opportunities for collaboration between researchers working on related projects.

> *Would a researcher be able to contact the first team to see if they could collaborate if they were going to do something slightly different?"*

Theme 6. Commercial Research and Competitor Collaboration: Specific considerations are raised about how the system would manage research requests from competing entities, particularly in the context of sensitive research such as pharmaceutical studies. This includes addressing potential conflicts of interest and ensuring fair access to data.

> *What happens if you've got, like, drug companies that are doing research and their competitors? And they don't want each other to know what each other's doing?"*

These themes collectively illuminate the need for this robust and transparent process that ensures both data security and responsible access. Balancing accessibility with stringent validation procedures and maintaining independence in oversight are critical elements to consider in the development and implementation of the system. In general participants are supportive of the concept and the moves to implement the 5 Safes. They did express that the materials are still vague about the who and the how and that they still have concerns about whether this is possible to achieve, including very healthy scepticism about how this will be funded and maintained.

Appendix

FOCUS GROUP DEMOGRAPHICS

This report is based upon three focus groups each containing 8 participants. The follow charts are a breakdown of demographic detail about those participants