

Too much information? Key considerations for vulnerability data-sharing

Summary

- For those of us with mental health problems, telling an essential services firm - like a bank or energy supplier - about our condition or needs can be difficult. Despite the additional help and greater accessibility it can lead to, only a minority of people with a mental health problem have ever 'disclosed' to those firms.
- Government bodies and others are exploring 'tell us once' systems, which would mean a customer only has to disclose their needs or condition once, with the information about that customer then being shared between other organisations.
- While such a service could make disclosure less taxing and ultimately get more support to those who need it, there are important issues that must be explored before these ideas are developed at scale.
- Understanding why only a fraction of people with mental health problems currently disclose to essential services firms is a first step. People with mental health problems have told us they don't believe it would make a difference and that they are concerned about how the information would be used, for instance in credit decisions.
- There are vital technical and legal questions that need to be addressed but if lived experience isn't central to its design, it risks leading to a service that, at best, doesn't make the most of the opportunity but, at worst, could discourage people from sharing their needs and becoming a costly failure.

Sharing data on customer vulnerability between organisations is under discussion

As debates about artificial intelligence, facial-recognition software or hacking of sensitive information show, how data is managed is central to many of today's most controversial issues. At the heart of those controversies is the challenge of taking up the opportunities that innovative uses of data offer while protecting people against the threats it can pose.

That challenge is evident when it comes to how data on your needs and potential vulnerabilities is gathered and shared. Within essential services like energy and financial services, recent developments have sparked new interest in this issue:

- In a speech in April 2023, the CEO of Ofgem, the energy regulator, spoke about a “tell us once” system, “where families who have vulnerabilities tell one agency about this and, with their permission, this is shared across all others with a single, reliable source of data to anticipate, identify, and respond to the needs of those customers.”¹
- The development of Support Hub, a tool created by Experian offering a ‘tell us once’ service to customers with support needs, allowing information to be shared with firms who have signed up to the service in one go.
- Work on the future of Open Banking, which is built on data-sharing, continues, with the future infrastructure and funding model being explored.
- The progress of the Data Protection and Digital Information Bill through parliament.

If handled well, these initiatives could lead to a world in which it's easier for people to share their needs and have them acted upon, to ensure that all of us have positive experiences when using essential services. But these developments also raise fundamental questions about how much control sits with the consumer, as well as around privacy, security, consent and whether it really helps to deliver improved outcomes.

In this short paper, we consider some of the benefits and risks of increased sharing of vulnerability data. While ‘tell us once’ systems would also need to be designed with customers with physical or other cognitive conditions in mind, here we focus on needs related to our mental health. To do that, we draw on past Money and Mental Health research as well as a new survey² of our Research Community, a group of 5,000 people with lived experience of mental health problems.³ Using that evidence, we outline key considerations that must be at the heart of data-sharing initiatives from the very beginning.

¹ <https://www.ofgem.gov.uk/news-and-views/blog/jonathan-brearleys-speech-ofgems-vulnerability-summit>

² 182 respondents, carried out over 3-13 November 2023.

³ All quotes in this paper are from that November 2023 survey.

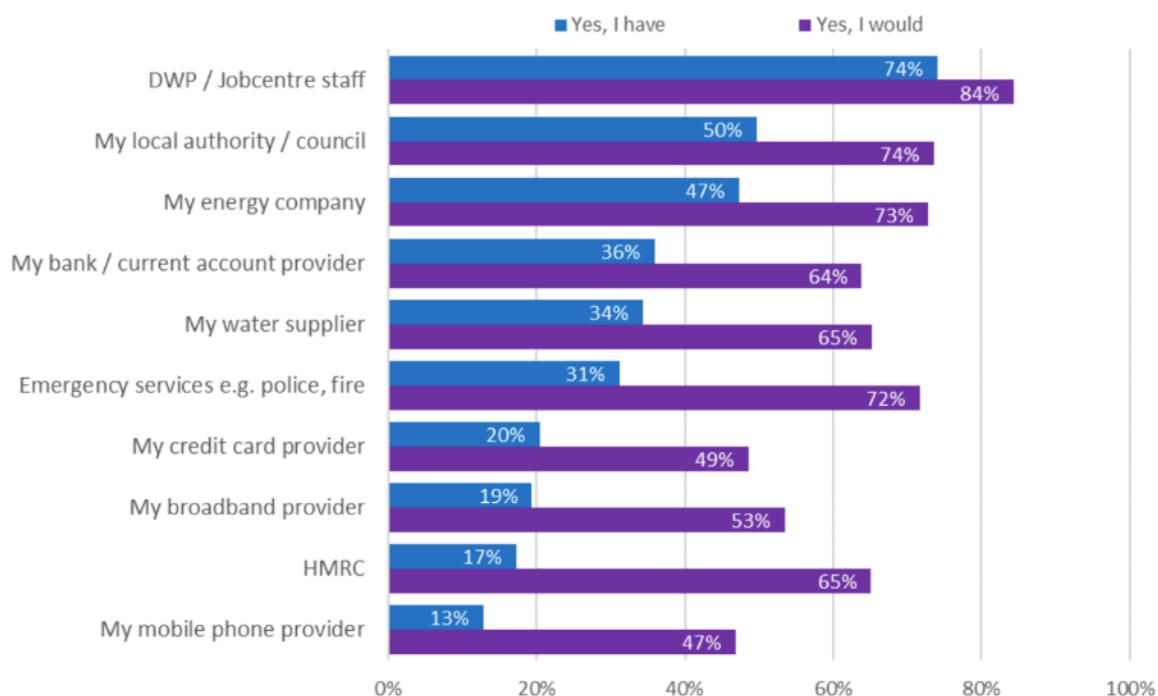
Most people don't tell essential services firms about their mental health problem

Systems to help customers with additional needs get support aren't a new development. This is most often done directly, with the customer telling their service provider, for instance a bank or energy supplier, what they need or discussing reasonable adjustments. But in a representative poll of people with mental health problems that we commissioned in 2021,⁴ we found that only a fraction of respondents had ever 'disclosed' their condition or needs to an essential service provider. Just 11% of customers with mental health problems had ever disclosed to their water company, with 12% having disclosed to their energy company, 13% to a telecoms firm and 14% to their financial services provider.⁵

To understand both people's past behaviour and their openness to sharing their mental health problem with an organisation in the future, we asked Research Community respondents both whether they *had ever* told their service provider about their mental health problem, as well as whether they *would ever* consider it. Among respondents, past disclosure levels were a little higher than our 2021 polling, as Figure 1 illustrates.

Figure 1: Respondents' appetite to disclose a mental health problem varied significantly across sectors and products

Have you ever told/Would you ever tell the following organisations about your mental health problem?



Source: Survey of Money and Mental Health's Research Community, carried out 3-13 November 2023. Base for this question: 178.

⁴ Bond N and D'Arcy C. The state we're in: money and mental health in a time of crisis. Money and Mental Health. November 2021.

⁵ Ibid.

Figure 1 also tells us about a wider set of organisations than we asked about in that previous polling. We broadened the scope because discussion of data-sharing - including through the concept of a universal Priority Services Register - has begun to consider other institutions beyond firms who could benefit from access to such data. This includes the Department for Work and Pensions (DWP), HM Revenue and Customs, local authorities and emergency services. It is perhaps unsurprising that DWP is the organisation that the highest proportion of respondents have disclosed to, given assessment for certain sickness or disability benefits depends on having a health condition. Something similar may be true for local authorities, in order to receive council tax discounts, grants and social care.

Understanding what drives the current low level of disclosure to individual firms, particularly in some sectors, is a crucial first step before considering joining up vulnerability data across firms.⁶ Our past research and most recent survey in November 2023 point to a number of different factors, summarised below.

Don't believe it would make a difference

A common reason why many people with mental health problems choose not to disclose is the perception that doing so would not have a positive impact on them. For some, this may be due to their mental health being 'under control', with their symptoms only rarely making standard services harder to use. But in our recent survey as well as our past work on disclosure,⁷ we also heard from many respondents who had little sense of what changes a firm could make that would help them.

For others, there was a more fundamental lack of confidence in some essential services firms, feeling that the companies didn't care enough about their needs to adjust their services in a meaningful and reliable way.

"The companies [that I wouldn't ever disclose to] are singularly geared towards profitability. In my experience, their staff are poorly trained to support customers with mental and/or physical health issues." Expert by experience

Past negative experiences and fear of judgement

While societal awareness and understanding of mental health problems has improved in recent years, a stigma remains. Research Community respondents shared difficult interactions they had had after telling someone about their mental health problem, including with staff in essential services firms.

⁶ Getting disclosure or data-sharing right won't solve the challenges encountered by everyone with a mental health problem. Some people will always choose not to discuss their mental health while over a third of people with a common mental disorder like anxiety or depression have never received a diagnosis. That's why making mainstream services as accessible as possible remains vital.

⁷ Fitch C, Holloway D and D'Arcy C. Disclosure environments: Encouraging consumers to disclose a mental health problem. Money and Mental Health and Money Advice Trust. November 2022.

“I don't feel safe disclosing that information. I feel like people treat me like I'm stupid or can't be trusted to handle my own finances rather than providing the appropriate support.” Expert by experience

Concerns at how the information would be used

In our most recent survey, the overriding concern raised by respondents was that sharing information about their mental health with organisations may lead to the data being used against them in the future. Above all, this related to decisions about access to credit, which may explain why only 49% of respondents had disclosed to their credit card provider.

“I would be frightened to tell a credit card company in case they declined me. I have had to rely on credit cards to pay my bills when I was on long-term sick and only receiving SSP [Statutory Sick Pay].” Expert by experience

“I feel my credit card provider may want to decline my having a credit facility, and this would impact my credit score or ability to manage finance if needed to use it urgently.” Expert by experience

For advocates of vulnerability data-sharing, none of these issues are insurmountable. In some ways, they directly point to an opportunity. For instance, for people who don't believe disclosure would make a difference to them, a service which could more clearly identify what support is available and what services can be adjusted could be transformative. And for those of us who have had bad experiences with disclosure, being required to do it once and only once could reduce the anxiety experienced when preparing to share this information. But without taking seriously the past negative experiences and broader worries about data use, there is a risk that such services fail to get sufficient buy-in from some of those who could potentially find it most helpful.

Views on Priority Services Registers

Beyond sharing directly with firms, one of the most common forms of logging consumers' vulnerabilities today is on a Priority Services Register (PSR). These are in essence lists that exist for energy and water consumers, and focus on identifying households who are most likely to struggle when there's a disruption to service, like a power cut, in order to get support to them. As recent research has shown,⁸ the information asked for in the energy PSR is neither standardised across organisations nor comprehensive.

The results of our recent Research Community survey illustrate both the potential and the current missed opportunity of PSRs. Nearly two-thirds (64%) of respondents are now or have ever been registered on a PSR. Among those, 47% said being on a PSR had had a positive impact on them, while only 5% said it had had a negative impact.

⁸ <https://www.helpfirst.ai/blog-posts/mapping-the-psr>

“It meant the method of communication was what I could manage; no phone calls, no unnecessary letters, just email communication.” Expert by experience

Considering the common doubt that disclosure would not bring any benefit, it's interesting to note the 48% of respondents who said being on a PSR hadn't had a positive or negative impact for them.

“Being on the Priority Services register made no difference whatsoever. I was not treated any differently.” Expert by experience

“It had minimal benefit for me as no one asked about my disabilities, I never had a water related emergency so none of the promised benefits materialised, and I was still financially exploited by the water company as they failed to notify me of the 50% discount I would have been entitled to had I been made aware of it and had I been offered help with the application form.” Expert by experience

Expert by experience perspectives on vulnerability data-sharing systems

Having established respondents' views on disclosure to individual firms or PSRs, we next turned to the attitudes towards vulnerability data-sharing services. We asked respondents what principles they would prioritise, capturing some - though not all - of the key considerations. Respondents were asked to rank the following statements from one to seven, with one being the most important consideration and seven being the least important:

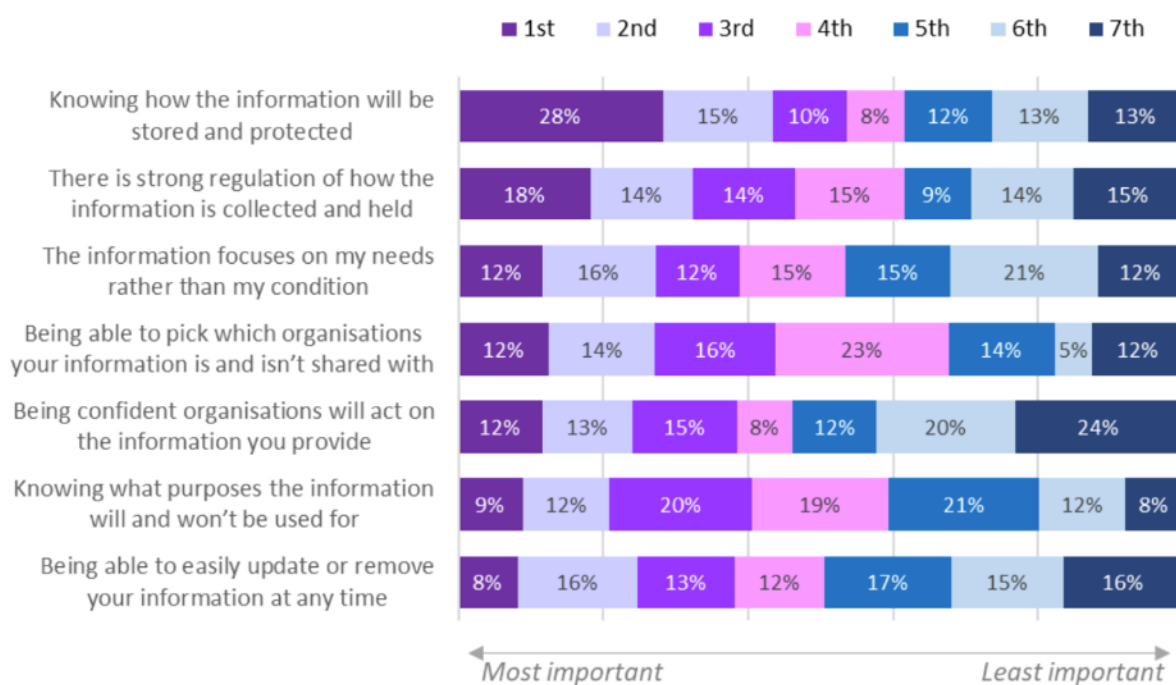
- Knowing how the information will be stored and protected
- Being able to easily update or remove your information at any time
- Being confident organisations will act on the information you provide
- Being able to pick which organisations your information is and isn't shared with
- Knowing what purposes the information will and won't be used for
- The information focuses on my needs rather than my condition
- There is strong regulation of how the information is collected and held

The single most important issue for respondents was “Knowing how the information will be stored and protected”. This was the number one priority for 28% of respondents, and number two for another 15%. The second-highest ranked issue was that “There is strong regulation of how the information is collected and held”, which 18% gave as their top priority and another 14% placed second. The least important issue for respondents was “Being confident organisations will act on the information you provide”, which 24% of respondents placed seventh and another 20% positioned in sixth.

But, as Figure 2 shows, each of the issues were a priority for a significant minority. “Being confident organisations will act on the information you provide” had the fewest respondents who chose it as a top priority, but it was still in top three priorities for 40% of respondents. This underlines that addressing a wide range of issues - as well as others we did not ask about, such as lived experience involvement - will be needed to build trust and uptake.

Figure 2: While prioritising how information is stored, protected and regulated, a wide range of concerns were important when it came to a vulnerability data-sharing service

Thinking about potentially using a service like that, how important would the following be to you? Please rank in order of their importance to you.”



Source: Survey of Money and Mental Health’s Research Community, carried out 3-13 November 2023. Base for this question: 180.

Notes: The full question asked of respondents was: “It has been suggested that it should be made easier for information about someone’s needs - including due to their mental health problems - to be shared between different organisations that provide essential services. This could be through one central service where the information is collected and then shared or by providers sharing the information with each other. Thinking about potentially using a service like that, how important would the following be to you? Please rank in order of their importance to you.”

What an ideal system would look like

In order to understand in more detail what respondents would want from such a service, we asked an open question on what people would want in an ideal world. While a number of themes emerged repeatedly in their answers, there were sometimes a diversity of views rather than a single clear preference:

- Who runs it - a number of respondents felt that the service should be done through one central hub, with many wanting this to be run by the government. Others wanted it to be independent but for it to be tightly regulated
- How the data should be managed - respondents wanted there to be transparency about how the data would be stored and used, and that the data would be secure and only used for the purpose of providing support. Some wanted to be periodically reminded of the service so they could make an informed choice about updating it or not
- What should be shared - there were a range of views on whether respondents would like to share needs, diagnoses or both. Others wanted more contextual information, such as experiencing a significant life event, to be shared
- How the data would be added - beyond the individual sharing the data, some said they would like a third party, such as an advocate or charity, to be able to add the information on their behalf
- Who it's shared with - a number of respondents felt it should be a mandatory requirement for firms in essential services to sign up
- Accessibility - respondents felt the process should be easy to complete and understand. There was a general preference for the service to be online but several wanted the option to be able to speak to a real person (online or over the phone) and for the process to be supportive and understanding. Crucially, respondents wanted it to be done once, rather than multiple 'tell us once' services
- What happens after sharing - as well as putting the request into action, some respondents wanted a confirmation or other follow-up from their providers after adding their information to the service.

A selection of Research Community views on a vulnerability data-sharing service

"I would need to either be able to complete my information in person, or preferably online... Essential services could then have access to relevant parts of it after safety checks that they would not misuse it."

"A central register sounds good, should be statutory so no organisations can opt out. Needs to be accessed by phone etc not just online. You need to see a copy of your entry and have regular reminders of who has accessed it. Should not be used for sales and marketing ever."

“Different services could then sign up to be part of it and receive updates about its customers. We could then pick yes/no for which services we want our central information to be shared with.”

“A simple, streamlined service would be great with login & password, a simple form where you can add / delete organisations, tick box and text box for health information. Privacy and confidentiality agreement in place so no third party gets access to the information unless permission is given.”

“I would like to... [b]e able to access this through more than one point of entry such as both online and apps (let's not rely solely on apps). Importantly, rather than solely having a list of diagnosis, have an area called ‘How I can be supported’ - which allows you to amend this as needed because depth of support can fluctuate.”

Concerns about vulnerability data-sharing services

After discussing an ideal system, we next explored respondents' worries or concerns. These centred on three key themes.

Retaining control over your own data

Respondents understandably wanted to retain control over who can access the information they share and when.

“Some organisations don't need to know certain details. I would like to have control over which organisations have access and to what information they can see.” Expert by experience

For some, they noted that their experience of poor mental health can be a one-off, episodic, recurring or persistent in nature. This made it crucial that any information shared should be sufficiently flexible and the decision to share reversible.

“I think it's important to highlight the non-linear process of a mental health problem which means it can involve episodes rather than a permanent state. An understanding akin to remission in cancer survivors.” Expert by experience

People with mental health problems can have difficult histories when it comes to information recorded about them. Respondents spoke about experiences of health services, specifically recording information which was inaccurate or outdated, with this information still influencing their experiences with services today. These examples were used to underline the importance of people having complete control over what data they

share, with whom and when. Respondents felt strongly that they should have the ability to remove data in real-time and that this should lead to that information also being deleted from organisations' own databases too.

Data security

Respondents expressed concerns about the trustworthiness of the organisation managing their data, specifically that information might be sold to other companies.

“It sounds good in theory, but I like to have control over where my information is used and is shared. I would be concerned that my information was inadvertently shared with an organisation I would prefer not to. The more organisations it is shared with, the more potential for it to go missing or go to the wrong place.” Expert by experience

Others expressed concerns about how the data would be stored, that this could be hacked, or sensitive data on potentially hundreds of thousands of vulnerable people could fall into the wrong hands, such as scammers.

“The fear that company data protection controls aren't top notch. And scam callers could take advantage of vulnerable people.” Expert by experience

Firms not being well-equipped to follow-through

Respondents reported that they lacked trust in firms' and individuals working within firms' ability to understand their needs arising from their mental health problems.

“[T]here can be a tendency for certain individuals to assume you are as thick as two short planks and accordingly act in a very condescending manner which exacerbates rather than eases situations.” Expert by experience

Respondents worried that, as with any recording of vulnerability, it ultimately comes down to the skills of the staff member seeing that information to adjust their approach according to a customer's needs.

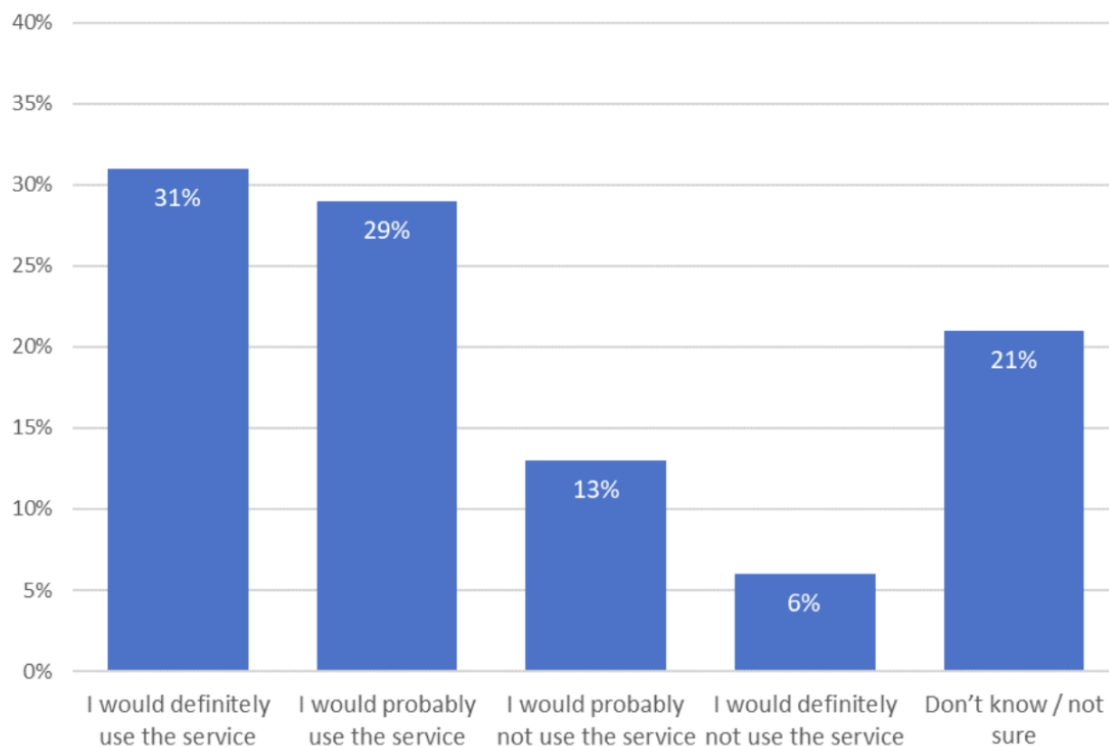
“The main concern is that if [information] is 'generally' shared then it is open to those you communicate with in first contacts with call centres etc. Most people that you encounter give the 'lip service' of stating we understand but actually have no idea. This is a real barrier as you then are left feeling guarded around judgemental attitudes as many seem to automatically be judgmental and assume your capacity etc is questionable.” Expert by experience

Likelihood of using a service like this

After ranking priorities and considering an ideal service and the potential drawbacks, we finally asked respondents how likely they were to use a vulnerability data-sharing service. This is a difficult question to ask and answer, as we did not specify a specific model of a service or how it would be managed and delivered. As the rest of this note has demonstrated, these are very important considerations. With that caveat, Figure 3 shows that a majority of respondents said they would probably (29%) or definitely (31%) use a vulnerability data-sharing service.

"I would find it much easier to only have to tell one service about any of my health conditions as I still, after 70 years, find it so very hard to bring the subject up. Once it is on the table I can discuss and inform easily." Expert by experience

Figure 3: While a majority of respondents would use a vulnerability data-sharing service, a significant minority would not or were unsure
"Overall, would you personally use a service that allows different essential service organisations to share information about your mental health with your permission?"



Source: Survey of Money and Mental Health's Research Community, carried out 3-13 November 2023. Base for this question: 182.

But Figure 3 also shows that a significant minority of respondents were less convinced. While only 13% said they would probably not use the service and 6% said they would definitely not use it, another 21% answered "don't know / not sure". As noted in our caveat above, this may well be because of the uncertainty about what a service would look like in practice.

There remain many unresolved questions

That uncertainty is inevitable in what was a short survey about an idea that is, for the most part, still in development. But it highlights the necessity for further, in-depth research as work on these topics continues. Above all, this paper has aimed to introduce the voices of people with lived experience into the discussion of this issue, which can sometimes feel as if it is primarily focused on technical or legal questions, rather than what the end-users ultimately want and don't want, and what their needs are. National Audit Office reports and analyses of government IT failures have frequently demonstrated how such projects can run aground. Focusing primarily on whether a service can be delivered, rather than grounding its development in the needs, concerns and challenges faced by its ultimate users, is likely to lead to an ineffective service, and most likely a waste of public money.

That is not to dismiss the importance of some of those legal questions. As was repeatedly raised by Research Community members, the ability to opt out of sharing data, either altogether or with certain organisations, is paramount to gaining people's trust. But there remains the potential that a firm can use elements of existing data regulations, particularly GDPR, to override that request if it feels that it has legitimate grounds to. Clarifying under what basis firms should be gathering, recording and sharing this information is vital to avoid a world in which organisations gather more sensitive data than people are comfortable with, undermining some of the great opportunities presented.

The technical considerations are key too, but again, should be built upon the needs of consumers. These questions include whether participating organisations should have to use standardised forms for recording vulnerability and then pass that onto the service so there's no wrong front door, or if firms should be able to tailor their approach to vulnerabilities with their own customer base. Similarly, acknowledging varying appetites to disclose to different organisations and considering the different harms people might be exposed to, public views should be sought on whether forms should look different from one sector to another.

While not the number one priority for Research Community respondents, understanding and managing expectations about follow-through and what's actually achievable by firms off the back of a disclosure will be crucial.

We have primarily considered this issue from the point of view of people with mental health problems. For people with physical health problems, or both physical and mental health conditions, different questions may be equally in need of further exploration and lived experience insight.

With so many unresolved questions, this is a topic we plan to return to in 2024.⁹

⁹ To get in touch about our work on this subject, please email Chris Lees: chris.lees@moneyandmentalhealth.org