

A once in 25 years opportunity:

ten principles for designing vulnerable
consumer data-sharing programmes

May 2024

This paper was written by a group of authors who have been involved in work on data-sharing, vulnerability, and disability over the last decade.

Each author has contributed to this paper in an independent capacity.

The paper is supported and distributed by WhatWeNeed.Support and the Money Advice Trust.

Contents

Authorship	3
A. Data-sharing: importance and opportunity.....	4
B. Debate: what are people saying?.....	6
C. Design: what principles should guide us?.....	13
Principle 1: speak the same language (define ‘data-sharing’, ‘disclosure’, ‘vulnerability’).....	15
Principle 2: data-sharing needs data (so avoid the known barriers to consumer disclosure) ..	16
Principle 3: this is not a technical project (keep the focus on solving the human problem)	18
Principle 4: ‘actionable support needs’ are the key (rather than higher-level flags alone)	20
Principle 5: consumers want to feel in control (even if some decide to never exercise this) ...	22
Principle 6: consumer data-sharing portals must be accessible (a key test of our values).....	24
Principle 7: consumer data-sharing portals should lead to support (accessible and timely) ...	25
Principle 8: organisations will use shared data differently (transparency is therefore vital)....	26
Principle 9: organisations in a sharing network don’t need the same lawful base	27
Principle 10: meet current need, watch for future harm (avoid unintended consequences) ..	28
D. Deciding: how do we take the opportunity?	29
Author biographies	30
Appendix 1 – vulnerability definitions	32
References	33

Authorship

This paper was written by Chris Fitch, Christine Tate, Dan Holloway, Elizabeth Blakelock, Faith Reynolds, Jo Giles, Johnny Timpson, Kevin Still, Lee Healey, Shani Dhanda, Steve Crabb, and Vanessa Northam.

This group have all been involved in work on data-sharing, vulnerability, and disability over the last decade, and have each contributed to this paper in an independent capacity.

Full author biographies and conflict of interest statements are found at the back of this paper. The views of the authors are their own and do not represent those of the organisations with which they work.

Money Advice Trust

This paper is distributed by the Money Advice Trust. The Money Advice Trust run a consumer vulnerability programme that has worked with over 350 firms, more than 35,000 staff, and across all regulated sectors: www.moneyadvice.org/vulnerability

WhatWeNeed.Support

This paper is also distributed by WhatWeNeed.Support. This is an open-source website that:

- collates and lists some of the changes, reasonable adjustments, and support needs that disabled and vulnerable consumers want firms, businesses, and institutions to meet
- describes them in such a way that organisations are able to act on them
- allows disabled and vulnerable consumers to add, contribute, and improve these lists so they cover a more accurate and wider range of needs and adjustments.

www.WhatWeNeed.Support is the web address of this initiative. It is run by Dan Holloway and Chris Fitch and is funded by a seed-funding grant from Experian's Support Hub Team to improve knowledge and practice on support needs.

Accessible publication

This paper has been designed to be accessible for as many disabled and non-disabled readers as possible. But, if the paper is not accessible to you, please tell us and we will seek ways to do better in the future. You can contact us at info@WhatWeNeed.support

A. Data-sharing: importance and opportunity

Introduction

This paper is about vulnerability, disability, and data-sharing across the essential service sectors.

It has been written to help make it possible:

- for vulnerable or disabled consumers to disclose and share their circumstances and support needs with multiple organisations through one simple process
- for essential service organisations to transparently share information about consumer circumstances and needs between themselves and other relevant bodies
- and to use such data-sharing to prevent and minimise harm, disadvantage, loss, or exclusion among these consumers in emergency situations and everyday service use.

Importance

An essential service is something that consumers **cannot do without** to live their everyday lives. These include financial, energy and water, phone and internet, postal and delivery services.

There is currently a national policy debate about increased data-sharing among essential services. This debate is critical – as BOX 1 shows - to millions of disabled and vulnerable consumers:

- who rely on multiple organisations to provide services that are literally essential or central to their ability to live and function on a daily basis
- who live in complex circumstances, with extra support needs, or with additional requirements that essential services need to know about and take into account
- who do not – because of their situation - have the resources, energy, or time to disclose their circumstances or support needs to each essential service in their lives in turn
- who therefore do not receive essential services - in both emergency and everyday contexts – that are accessible, usable, beneficial, and optimal.

We have known this for years. And for years, commentators have called for a simple process – often called **‘Tell Us Once’** - to allow information about consumers’ situation and needs to be easily disclosed and shared with multiple essential services.

Opportunity

Due to a series of events (see SECTION B), these long-standing calls have started to be acted on. Consequently, we have a ‘once in 25 years’ chance to introduce a system that can change lives.

To achieve this, however, we will need this new system to not only be informed by technical or legal insight, but also the **voices, needs, and experiences of vulnerable and disabled consumers.**

This paper therefore proposes **10 key principles** – drawn from research, policy, and lived experience - to ensure this critical balance is struck, and that the right data, are shared in the right way, and with the right outcomes for consumers and essential services alike.

BOX 1

The consumer challenge

Among the **54 million adults** in the UK, approximately:

- **14 million** are disabled¹, **25 million** are vulnerable², **4 million** are unpaid carers³
- around **40%** of disabled adults feel they are unable to access or use many essential services because these do not offer the support or reasonable adjustments they need⁴
- **70%** vulnerable consumers report issues in interacting with their service provider due to a health condition, while **23%** indicate similar issues due to a negative life event⁵

Despite this, among some vulnerable and disabled consumers:

- only **11-14% have ever disclosed** a need for support to any essential service provider⁶
- **30-70%** report complex, lengthy, or 'pointless' processes that can **deter disclosure**⁷
- many indicate **inaccessible channels** make disclosure difficult, if not impossible⁸
- and where **consumer worry** about data usage and onward sharing is a key barrier⁹

Taken together, this means:

- **within essential services**, only a minority may ever receive a consumer disclosure
- **in disabled and vulnerable consumers' lives**, support needs are often not disclosed or met
- **across essential services**, data-sharing could help such needs to be known and met
- **consumer worry** exists about transparency, control, and sharing of their data.

Key terms

- **Vulnerable consumer** - consumers that (a) could become vulnerable in certain situations to specific harms, disadvantage, losses, problems, or exclusion from services unless (b) action is taken at the right time by their essential service organisations to understand, prevent, and respond to such harms (see Appendix 1 for sector definitions).
- **Disabled consumer** – consumers with a physical or mental impairment that has a substantial and long-term effect on their undertaking everyday activities, and where reasonable adjustments may be needed to access, use, and benefit from essential services
- **Essential services** – services that consumers need to live their everyday lives (including financial, energy and water, phone and internet, and delivery services).
- **Disclosure** - where something often private or personal is shared by someone. It is a vital moment of trust for consumers, an opportunity for firms to take the right action, and for data sharing networks to overcome any barriers of doubt and fear.

B. Debate: what are people saying?

Key voices

Four key voices in any debate on disclosure and data-sharing are those of vulnerable and disabled consumers, essential services themselves, their regulators, and UK Government.

B1. Disabled and vulnerable consumers

As outlined in PRINCIPLE 5, disabled and vulnerable consumers may welcome data-sharing for greater levels of understanding or support, but **not at the cost of transparency and control** over how their data are shared. This perspective is **central to the principles** in this guide.

Of particular note here, is that most (although not all) of the data likely to be shared on disability or vulnerability will **be derived from disclosures made by consumers themselves**.

Consequently, a level of consumer interest exists in dashboards, portals, and solutions that allow them oversight, control, and choices over these disclosures, their data, and its sharing.

This does not mean that every consumer will want to ‘micro-manage’ their information. Nor does it mean that essential services will never share information - such as in ‘life or death’ or other relevant situations - without a consumer directing this. But it does reflect the strong emphasis that many consumers place on involvement, choice, and autonomy.

B2. Essential services

Essential service organisations, **in an individual capacity**, have been recording disclosed data about disabled and vulnerable customers’ support, safety, communication, and access needs for over a decade. However, the sharing of these data **between organisations** is more recent.

Individual **energy and water firms** in England, Wales, and Scotland for example, already record disclosed data about customers with extra support needs. Stored on each firm’s ‘Priority Services Register’ (PSR), initial work has been undertaken to now start sharing these data between energy and water companies (**BOX 2**).

Meanwhile, in Northern Ireland, a separate ‘Care Register’ scheme for energy and water firms is in operation, with plans for greater data-sharing between these sectors being put into place from 2024 onwards .

Notably, work on PSR data-sharing in the energy and water sector has underpinned the recent call in April 2023 by Ofgem’s Chief Executive (Jonathan Brearley) for vulnerability data-sharing with other sectors such as telecommunications, financial services, and local and national government. The scope for creating such a **Universal Priority Service Register** is now being explored by the Government’s Department for Business and Trade (see **B4**).

BOX 2: ENERGY, WATER, AND THE PRIORITY SERVICES REGISTER¹¹

The Priority Services Register is a free service in England, Scotland, and Wales which provides consumers with extra advice and support, including during interruptions to electricity, gas or water supplies.

Each energy and water firm encourages consumers who require extra help to share their situation (from a fixed list of categories known as 'needs codes'). Support is then tailored and services provided to eligible and registered consumers in everyday and emergency situations.

Pre-2000

- **1990s** - energy/water firms operate their own lists of customers requiring extra help
- **1999** - these lists (all differently named) are retitled as the 'Priority Service Register'

2000-2009

- **2000** - the PSR operates as a voluntary scheme for energy firms
- **2008** - Ofgem make the PSR mandatory | Ofwat encourage water firms to adopt it

2010-2019

- **2015** – creation of Safeguarding Customers Working Group (networks, suppliers, independents, and relevant bodies such as consumer, trade, regulatory and charities) leads to first steps in joining-up separate PSR registers and establishing data-flows
- **2016** - Ofgem and SCWG collaborate to expand the range of situations recorded by the PSR, with a requirement for firms to promote and register more people on the PSR
- **2017-18** – SCWG electricity and gas members align needs codes, improve data-flow arrangements, establish data protection basis for sharing (including the 'PSR promise')
- **2018** – initial meetings are held between SCWG and water sector to explore potential for sharing between energy and water
- **2019** - energy and water firms test existing 'needs codes' to establish potential for data-sharing between sectors

2020 onwards

- **2020** - common set of needs are adopted and used by firms (including 'justification matrices') to shape consistent set of accompanying support actions
- **2020-21** - Ofgem, Ofwat, and ICO engage on the appropriate legal basis for data sharing
- **2023** (April) - data-sharing between water and energy distribution networks begins
- **2024** - ongoing work to include other energy participants (including Gas Distribution Networks) in PSR data-sharing begins

In the **financial services sector**, separate firms or company groups typically do not share data about a customer’s vulnerability or disability situation with each other. However, there has been a growth in firms receiving data from ‘Tell Us Once’ portals where consumers can share their own support need information with multiple firms through a single process or ‘gateway’. The largest of these portals is Support Hub by Experian (**BOX 3**). In addition, there are also systems – such as Morgan Ash’s MARS and Comentis – that enable firms to assess consumers’ vulnerability to different forms of harm (such as a health situation or ability to make a specific financial decision) and then recommend actions to mitigate those harms.

Among **telecommunication firms**, we are not aware of any data-sharing arrangements either directly between firms or using consumer-driven ‘Tell Us Once’ systems. However, some types of firms are required by Ofcom to offer a ‘priority fault repair’ service to disabled customers, incapacitated and housebound individuals, and households with a severely ill child.

Meanwhile in the **Local Authority** space, the Vulnerability Registration Service portal allows for the sharing of high-level vulnerability flags with selected authorities, while TellJo provides a service individuals can use to disclose support needs with individual local authorities and housing sector organisations.

Finally, there are some Tell Us Once systems that focus on **bereavement and death notification**, with these including (in alphabetical order) Death Notification Service, Life Ledger, Notify Now, Settled, and the Gov.UK platform for disclosing a death to multiple Government departments.

B3. Regulators

Regulators expect firms to facilitate consumer disclosure to achieve better outcomes and experiences. Some regulators also encourage the exploration of vulnerability data-sharing arrangements between different organisations to potentially better support consumers.

Ofgem

Disclosure: In their 2019 Vulnerability Strategy¹², the Office of Gas and Electricity Markets (Ofgem) - which oversees energy - set an outcome for firms to demonstrate they had made it easier for customers to ‘self-identify’ or disclose vulnerability. Importantly, specific reference was made to consumers being able to self-disclose. OFGEM added that “companies need to build trust and make sure that consumers are not penalised for self-disclosing”.

“We want to see evidence that there has been an improvement to support consumers to self-identify”
OFGEM, 2019

Data-sharing: Ofgem have also actively encouraged the sharing of data *within* the energy sector (between individual energy firms and larger network operators), between the energy and water sector (with sharing, where possible), and potentially *across other sectors* too in the future (including the NHS, councils, fire service, and third sector)¹³.

We should...consider building towards a joint register, not just...water and energy, but wider”
Jonathan Brearley, CEO, Ofgem, 2023

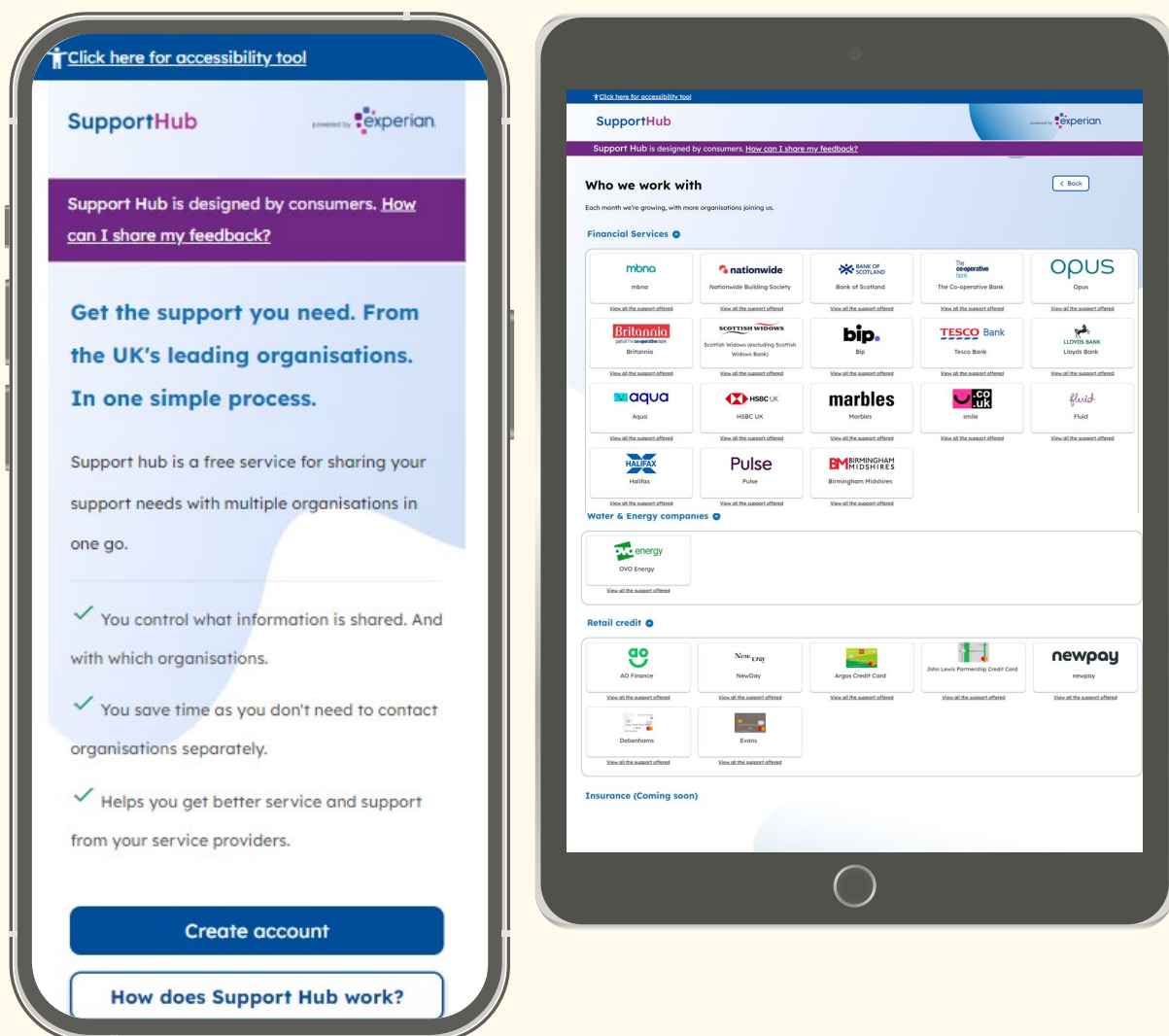
BOX 3: 'TELL US ONCE' IN THE FINANCIAL SERVICES AND ENERGY SECTOR

In the financial services sector, the number of regulated firms and range of services provided has meant that there is no mandatory equivalent of a Priority Services Register.

However, some of the largest providers of financial services in the UK are participating, alongside energy sector representation, in a 'Tell Us Once' system called 'Support Hub'.

This allows consumers to disclose their support needs to multiple firms in one process, but also to manage, update, revoke, and control the data they have shared with firms that they select.

Conceived in 2021, developed in 2023, and launched in 2023, Support Hub is more than an idea or proposal and is currently helping real consumers to share real support needs in real time with 26 large national financial services and energy brands.



<https://supporthub.experian.co.uk>

Ofwat

Disclosure: the Water Services Regulation Authority (Ofwat) have made statements about the need for firms to better identify customers in vulnerable situations. And in their “Practitioners’ Pack”, Ofwat notes that encouraging customers to disclose any vulnerable circumstances could provide a helpful strategy for firms¹⁴.

“it is useful to encourage customers in circumstances that make them vulnerable to disclose their need”
OFWAT, 2016

Data-sharing: Ofwat also support data-sharing arrangements. In their vulnerability guidance for firms¹⁵, Ofwat state that “companies should actively consider how they can reduce communication burdens on customer[s] who need extra help; [including] establishing data sharing arrangements with partner organisations”. However, Ofwat note that in doing this, firms should consult vulnerable customers to establish their views.

“In designing their approach to sharing... vulnerability data, companies should take into account customer views on data protection and privacy”
OFWAT, 2023

Ofcom

Disclosure: The Office of Communications (Ofcom) regulates companies providing telephone, mobile, broadband, postal and other services. In its “Treating Vulnerable Customers Fairly” guidance¹⁶, it recommends that firms do more to encourage customers to disclose their situation and support needs. It also notes that the signals and messages that firms send to consumers is key: “customers might be more willing to share information about a vulnerability if they know they can get extra support from their provider by doing so”. This approach has also been emphasised in Ofcom’s recent rules for postal operators¹⁷.

“Providers should encourage customers to tell them about any specific accessibility or customer services needs they have,”
OFCOM, 2020

Data sharing: Under Ofcom’s General Conditions of Entitlement¹⁸, some regulated telecommunication companies will offer a priority fault repair service for customers who depend on the telephone because of ill-health or disability (and have an urgent need for a repair). However, data on these customers are reportedly not shared with other companies, nor do plans exist to do this.

“Under [our] new rules, postal operators must have policies and procedures in place to ensure disabled customers can communicate their delivery needs to them, and firms will need to ensure couriers will meet those needs when delivering parcels.”
OFCOM, 2022

Financial Conduct Authority

Disclosure: The Financial Conduct Authority (FCA) - which regulates the financial services sector - expects firms to understand their customers' needs. It highlights encouraging disclosure as an important step towards securing that understanding. In its finalised vulnerability guidance, the FCA also notes that "firms should ensure that they are open and transparent...about how any information disclosed will be used"¹⁹.

"firms should...set up systems and processes in ways that will support and enable vulnerable consumers to disclose their needs"
FCA, 2021

Data-sharing: The FCA's regulatory stance is spelt-out in their finalised 'Guidance for firms on the fair treatment of vulnerable customers' (FG21/1): that firms should follow existing data protection legislation to ensure fair, lawful and proportionate data sharing, and that doing this appropriately may result in better consumer outcomes.

"Sharing data with third party individuals or organisations may be important in achieving good outcomes for a vulnerable customer"
FCA, 2021

Information Commissioners' Office

Disclosure: The Information Commissioner's Office (ICO) upholds information rights in the public interest, including those specified in the Data Protection Act (2018) and UK General Data Protection Regulation. This includes arrangements to manage, record, use, and share disclosures of personal or special category information (the latter covering more sensitive data - e.g. health information - that requires a higher level of care and processing actions).

"we need to even...[the] balance between those who hold our most precious data and the most vulnerable who hand over their data, often with little knowledge of their rights"
ICO, 2022

Data-sharing: As the ICO have a Code of Practice on what organisations should consider before sharing vulnerability data²⁰, this paper does not duplicate its content. However, it is worth noting that the ICO's Code asks organisations to consider five key questions: (i) what their aim in sharing data is; (ii) what risks this might pose; (iii) whether a lawful processing basis to share data exists; (iv) how the data will practically be shared, who with, and how consumer rights will be upheld; and (v) how organisations will evidence that their actual data sharing matches their original stated purpose. The ICO have also noted – in its ICO25 strategic plan – that they will also increasingly consider protections for, and the needs and wellbeing, of vulnerable people in their approach to regulation²¹.

"we will not tolerate organisations...using people's information to exploit them or expose them to harm, and we will not take action against organisations who share data to safeguard vulnerable people"
ICO, 2022

B4. Government

Universal Priority Services Register (2023)

In late 2023, the UK Government announced that it was exploring the creation of a single, multi-sector 'Universal' Priority Services Register²².

Working on a 'Tell Us Once' basis, such a Register would potentially allow consumers to share their vulnerability or support needs once, with data being shared across the regulated sectors of energy, water, and telecommunications (and possibly to other sectors in time).

While recognising recent improvements in the current Priority Service Register, the Government also highlighted long-standing limitations. These include an over-focus on drivers of vulnerability rather than actionable support, often unclear and inaccessible disclosure and information management journeys, and a limited range of participating essential services.

Consequently, as part of a wider consultation, the UK Government have called for fresh thinking and new approaches to data-sharing on vulnerability, with a written response due at the time of writing. This could incorporate current work on the 'Support for All' initiative led by Northumbrian water, as well as work in Northern Ireland (where the Utility Regulator is aiming to develop a Customer Care Register for domestic gas, electricity and water consumer), the Welsh JIGSO register for emergency services (of properties with at-risk vulnerable individuals), and work by devolved bodies such as Social Security Scotland and Scottish Water.

Data Protection and Digital Information Bill (2023)

In addition to the above exploratory work, the Data Protection and Digital Bill was introduced in the House of Commons in November 2023 (having been originally introduced in 2022, but then withdrawn to allow for further consideration and consultation)²³.

Due for Royal Assent in 2024 (where the Bill will become an Act of law), the Bill provides a framework for numerous purposes including sharing of customer data through **smart data** schemes to provide additional services to consumers (including personalised market comparisons and account management).

The Bill (and later Act) will have practical implications for the sharing of information from disabled and vulnerable consumers, and the principles outlined in this document should be considered in relation to this.

Digital Economy Act (2017)

The Digital Economy Act²⁴ covers issues of digital communication, infrastructure, and services, including data-sharing between public bodies to improve services. The Act outlines what information can be shared, for what purposes, and – via 'Codes of Practice' such as the 'Public Service Delivery, Debt and Fraud' code²⁵ - with what protections for individuals.

This latter Code of Practice makes specific reference to data-sharing to safe-guard vulnerable individuals. This includes sharing to identify and support individuals experiencing water/fuel poverty, or vulnerable individuals subject to debt collection. However, due to devolution and national legislative differences, parts of the Act only apply to selected UK nations.

C. Design: what principles should guide us?

Significant discussions are clearly taking place on vulnerability and disability data-sharing. In this paper, we outline 10 principles to help shape their design, development, and delivery.

Principle 1: speak the same language (define ‘data-sharing’, ‘disclosure’, ‘vulnerability’).

Discussions about data-sharing often result in misunderstandings (particularly between consumers and organisations). This is because the same words are often used to talk about different things. It is therefore critical to define key terms and common language.

Principle 2: data-sharing needs data (so avoid the known barriers to consumer disclosure).

Overlooking lessons from existing research and evidence will result in a system that is not only ineffective and unsupported by consumer engagement but could also negatively affect wider consumer attitudes and behaviour towards disclosure.

Principle 3: this is not a technical project (keep the focus on solving the human problem).

If we do not understand the core problem that disabled or vulnerable consumers (rather than essential services) currently have with disclosure, we may design a system that works for organisations and regulators, but not for the actual consumers we want to disclose.

Principle 4: ‘actionable support needs’ are the key (rather than higher-level flags alone).

If we do not share what specific form of support a consumer requires (and instead rely on flags that just indicate a support need exists), then each organisation in contact with a consumer will then potentially have to make contact with that consumer to understand what support actually does need providing – requiring this type of multiple contact is the direct opposite of a Tell Us Once system, and is avoidable through good design.

Principle 5: consumers want to feel in control (even if some decide to never exercise this).

Situations will arise where information could be shared ‘for someone’ in their ‘best’ or ‘vital interests’, and these situations need careful definition, explanation, and monitoring. However, in all other cases - until shown otherwise - disabled and vulnerable consumers should be presumed to have the capacity and interest in controlling their own data.

Principle 6: consumer data-sharing portals must be accessible (a key test of our values).

It would be not only ironic, but also damaging and demoralising if a portal for consumers to share their need for extra support was itself designed in an inaccessible or exclusionary way.

Principle 7: consumer data-sharing portals should lead to support (accessible and timely).

Clearly, where a consumer shares a need for support (which an organisation receiving this data has indicated it can meet), this should lead to that support and help being consistently given in a way that also takes account of other accessibility needs. For example, if a disabled customer needs advance notice of any interruption to supply, it is critical that this advance notice is not only given but is also communicated in the accessible format that a consumer may have also disclosed as an accompanying support need.

Principle 8: organisations will use shared data differently (transparency is therefore vital).

These different ‘purposes for processing’ (and any controls a consumer may have over this) need to be clearly communicated to consumers so they can decide to participate or not in any data-sharing arrangement. This is critical because as a ‘sharing network’ grows and new organisations join, these new entrant organisations may want to use data in different ways which consumers may not expect or understand (including the introduction of new uses, risks and consequences not previously anticipated or considered by consumers). This needs to be done in a consistent and accessible way to ensure that consumer trust in disclosure stays high.

Principle 9: every organisation in a sharing network does not need to use the same lawful processing base under the Data Protection Act (2018) for recording and sharing data.

While some data-sharing networks will use the same lawful processing base, this is not legally required by the DPA 2018 or the ICO. Furthermore, it is also not practically realistic to expect every organisation across different essential service sectors to use the same lawful processing base (and such an expectation may act as an unnecessary barrier to different firms or sectors participating in data-sharing arrangements).

Principle 10: meet current need, watch for future harm (avoid unintended consequences).

The test of any data-sharing scheme is not found in metrics relating to disclosure levels or volume of shared data, but whether a consumer receives the support they need at the right time and in the right way. Equally, any initiative involving data needs to consider not only its immediate and intended purpose, but also the potential future uses of this data. Importantly, this spans the recognised and perceived risks that disabled and vulnerable consumers may have about this (including its re-use by machine learning and artificial intelligence technologies).

Principle 1:

Speak the same language (define 'data-sharing', 'disclosure', and 'vulnerability')

Data-sharing discussions often result in confusion and misunderstanding because the same words are used to describe different things. It is therefore helpful to define these terms:

- **Data** - personal data is information about a living individual such as their name, address or birth date, but also includes their interactions or transactions with organisations. Special category data is information about a person that is more sensitive, requires higher levels of care, and includes a person's health situation (see PRINCIPLE 9).
- **Data-processing** - this covers almost anything that is done with data including collecting, recording, storing, using, analysing, combining, disclosing, deleting, or sharing.
- **Data-sharing** - there are multiple ways in which data can be shared (and re-shared):
 - **Tell Us Once** refers to an approach where consumers can share information with multiple and different organisations through one simple process or platform. This removes the need for repeated disclosure to each individual organisations in turn. Well-designed Tell Us Once systems not only allow consumers to share information like this, but also to manage, update, and delete this information at a later point.
 - **'Data pooling' or 'firm driven' systems** often still rely on a consumer disclosing and sharing, but once this has happened any organisation participating (or joining) the sharing network or 'pool' can access and view that shared data. A potential variant includes organisations being able to directly add information they already hold about 'their consumer base' to the pool (with other organisations being able to see this). In both approaches, consumers may not be able to control which organisations access information about them (or be made aware when this happens), and organisations may either be able to access data about any individual, or be restricted to individuals they have an existing relationship with.
 - **'Dynamic' data-analysis models** may be used in planning or responding to events, interruptions, or emergencies. Used to facilitate resource allocation or triage, they can involve firms bringing together a range of non-vulnerability data sources into their analyses (such as flood warnings or other event information), alongside disclosed vulnerability data.
 - **'Open Data' or 'Smart Data' approaches** allow a third-party service provider to access consumer data held by another organisation with the consumer's permission (e.g. 'Open Banking' where transaction data is accessed to provide a consumer with a financial service).
- **Disclosure - is where something often private or personal is shared by someone.** It is a vital moment of trust for consumers, an opportunity for firms to take the right action, and for data sharing networks to overcome any barriers of doubt and fear.
- **Vulnerability** - there are many definitions of 'vulnerability' (Appendix 1). However, regulators are increasingly converging on firms understanding (a) what harm vulnerable consumers are vulnerable to and (b) what support is needed to minimise or prevent this.

Principle 2:

Data-sharing needs data (so avoid the known barriers to consumer disclosure)

In contrast to the academic literature (where relatively little has been published), a larger volume of policy studies have researched both the prevalence of disclosure to essential services by potentially vulnerable or disabled consumers, and consumer reported barriers to disclosure.

This research has been concentrated among consumers with mental health problems and has drawn on non-random samples (in size from 30-5000 participants). In the absence of other research, caution must be exercised in extrapolating the findings to other consumer groups.

However, there are at least **three insights** from these studies that are potentially useful to those developing disclosure and data-sharing systems:

i. Historically, among such consumers, disclosure levels to essential services have been low

As **BOX 4** shows, in the largest study conducted to date, the Money and Mental Health Policy Institute (2021) found that, among 5000 survey respondents, only 11-14% reported ever disclosing their condition/support needs to an essential service organisation.²⁶

ii. Multiple reasons for such low levels of disclosure have been repeatedly documented

As **BOX 4** also illustrates, quantitative and qualitative research from MMHPI and also Mind^{27 28}, have repeatedly outlined the known barriers to disclosure. These include a lack of belief that support will be given, fear of poor treatment or negative consequences, and a lack of opportunities to disclose information or control how it will then be used.

iii. But disclosure levels - if lessons are learnt - do not have to remain this way in the future.

As **BOX 4** finally shows, we can use existing research to address the known barriers to disclosure. Furthermore, in the most recent research conducted (2023), many consumers with mental health problems reported to MMHPI a likelihood of disclosing and sharing if the right system is designed and put into place²⁹. Here consumers place an emphasis on transparency and security, strong regulation of collection and sharing, a prioritisation of actionable support needs (rather than recording conditions or causes alone), and consumer control over which organisations data are (and are not) shared with.

Clearly, designers of any data-sharing system should (i) **grasp the repeatedly given reasons for non-disclosure** by affected consumers and (ii) **address each of these barriers in turn** while designing any subsequent data-sharing platform or network. Furthermore, any disclosure platform or data-sharing system that does not address these barriers - and which is not transparent, does not offer controls, or does not allay concerns about the negative consequences of data-sharing - could negatively affect not just disclosure to the specific system itself, but also **wider consumer perceptions and trust in disclosure to other firms and sectors.**

In short, given data-sharing systems rely (mostly) on disclosed consumer information, we should not take any action which 'turns off' our already limited disclosure supply.

BOX 4: LEARN FROM THE PAST, DEVELOP FOR THE FUTURE

i. Historically, disclosure levels to essential service firms have been low among some vulnerable and disabled customer groups

Sector	% of respondents who report ever disclosing their mental health condition or support needs to a firm in this sector
Water	11%
Energy	12%
Telecoms	13%
Financial services	14%

Notes: this reflects earlier findings from MMHPI in 2016 (5500 participants), Mind in 2011 (878 participants), and Mind in 2008 (1804 participants), where consistently only a minority of respondents reported disclosing to essential service firms.

ii. Multiple reasons for such low levels of disclosure have been repeatedly documented.

Quantitative surveys from MMHPI and Mind have repeatedly outlined these barriers. These are listed in broad 'higher to lower' frequency order across the studies conducted:

- disclosure would make no difference
- dislike of sharing details of condition
- fear of not being treated sensitively
- concern about how disclosed information would be used
- worry about access to future services
- thought they would not be believed or would be treated unfairly
- embarrassed to share
- concerned about impact on benefits.

Notes: among the qualitative reasons given **for making a disclosure**, securing **practical change and support** was key, as well as having control over what disclosed data were recorded, used and shared .

iii. But disclosure levels - if these lessons are learnt - do not have to remain this way.

A sense of positive potential may be beginning to emerge among some consumers.

The most recent research from MMHPI (late 2023 with 178 participants) found:

- 47-73% would consider disclosure to an individual essential service in the future
- the top priorities to consumers in the design of a future data-sharing system were:
 - knowing how their information would be stored and protected (28%)
 - strong regulation of how any information were collected and shared (18%)
 - focus on the disclosure of needs rather than condition (12%)
 - controlling which organisations information was/was not shared with (12%).

Principle 3:

This is not a technical project (keep the focus on solving the human problem)

It would be easy for those involved in overseeing any data-sharing arrangement to focus on the many operational, legal, and regulatory challenges to overcome.

However, while these are challenges, they are not the central problem we need to solve.

Instead, the problem we need to solve (and organise around) is the essentially human one of recognising that on a daily basis millions of disabled and vulnerable consumers:

- rely on multiple organisations to provide them with services that are essential to their lives
- but will not - as disabled or vulnerable people - have the energy, time, and levels of trust to repeatedly disclose their support needs to multiple organisations (including having to follow complex processes or using inaccessible channels)
- and where consequently, disabled and vulnerable consumers simply do not end-up making or completing such disclosures to their essential service firms
- often resulting in these consumers receiving a service - either in periods of emergency interruption or everyday provision - that can be sub-optimal, inaccessible, and unusable, and which may result in other forms of more personal detriment, disadvantage, or loss.

Such a constellation of human challenges can be difficult to see when we think about just individual firms and how they might work to encourage disclosure or support consumers. However, as **BOX 5** illustrates (*“every repeated disclosure steals a week of my life”*), when we consider the manifold network of organisations that make up our lives as consumers, the impossibility of sharing and managing our support needs with these becomes crystal-clear.

Consequently, we must define our purpose and develop our design for data-sharing not only with our operational, legal, and regulatory specialists, but alongside the very consumers who are experiencing the social problem and harm we are trying to address.

If we do not, we may successfully share vulnerable consumers’ data over firms and sectors. However, it may not be the right data, shared in the right way, for the fair outcomes needed.

It is therefore critical to involve people with lived experience, and this requires more than consultation, or representation of their views through consumer or specialist charities but **embedding people with this lived experience within the core design team**. This ensures - in addition to the skills that individuals bring - that the central design problem to address is not overlooked, and that there is always lived experience in project discussions alongside technical, legal, and regulatory expertise. Importantly, this lived experience can be found both among consumers, as well as staff and employees of essential service organisations.

BOX 5:

DAN'S STORY: "EVERY REPEATED DISCLOSURE STEALS A WEEK OF MY LIFE"

I have bipolar disorder and ADHD. This means there are things I find very hard or impossible that others find inconvenient, or at worst, just don't notice.

Two of these things are phone calls and task sequencing. This makes it almost impossible for me to access many essential services where the default communication is by telephone, or I have to use multi-factor authentication to access vital documents or account details.

Many people on the other end of an email or webchat, or in a store, simply don't understand. So I have to spend a huge amount of time explaining. Other people think they do understand because they find these things "a bit inconvenient." And you can feel the judgement, of them thinking, sometimes saying "why can't you just cope with it like everyone else does".

Trying to interact with services that most people take for granted means having to make this kind of disclosure. Every time. That could be trying to access my GP or getting vaccinated; arranging delivery for something I've ordered online; trying to communicate with my electricity provider. And it's not just the experience itself, which is often traumatising, reminding me of being bullied or denied access in the past; making me give intimate medical information just to do something many do without thinking.

As well as that, every time I do this I have to prepare myself in advance so I can cope with that trauma. I need to do research to find out how I can make arrangements to ask for something accessible. I have to run through the scripts in my head to deal with replies from people who don't get it or don't believe me. And afterwards I feel distressed and exhausted. Not "tired." But unable to function. Sometimes for days. Every repeated disclosure steals a week of my life doing this.

And of course if I need to interact with two firms that week, one of them has to get ignored. So bills will go unpaid. Or I will buy something more expensive from a different firm. If something is broken, I don't return it. And I never get to switch providers.

This makes a huge financial impact. But it also means I miss out on doing the things other people get to do. The things that give their life meaning. Because I'm too busy preparing for, or recovering from, another disclosure.

***Notes:** Dan's story describes the experience of Dan Holloway (one of the author's of our report), but reflects a reportedly common situation among other disabled consumers.*

Principle 4:

‘Actionable support needs’ are the key (rather than higher-level flags alone)

An immediate first question that essential services often have in relation to vulnerability or disability is ‘what type of vulnerability/disability is involved?’. However, an arguably more effective question is ‘what is the consumer *vulnerable to*?’.

The reason for this is that while we might know a consumer has, for example, a physical disability or health problem (a ‘general support flag’) **this tells us nothing** about the actual support or reasonable adjustment to service provision that is needed.

Clearly, some commentators might respond that setting a ‘general support flag’ (such as ‘has physical health problem’) would allow any essential service organisation to simply contact consumers for an explanation of the underlying support need.

However, this goes against the fundamental principle of any Tell us Once system as:

- it usually requires every organisation the consumer uses to then contact that consumer (which, if a consumer has N relationships with N organisations, would involve handling multiple contacts, telephone calls, emails, SMS, letters, and other intrusions)
- forces the consumer to then explain their support needs to each one of these N organisations that contacts them (requiring multiple and repeated re-disclosures which takes time for the consumer and is a service cost for organisations)
- it assumes that disabled and vulnerable consumers could manage this process which (given their often lower levels of energy and resources) may be unlikely or unrealistic
- and it could ultimately lead to vulnerable and disabled consumers being overwhelmed, unable to engage, and potentially not receiving the service that should be (which itself could result in multiple forms of detriment).

Consequently, platforms that rely on general high-level flags are not Tell Us Once systems, and instead are more accurately described as ‘Tell Us Many’ systems.

In contrast, systems that do use actionable support needs (i.e. descriptions of what change or adjustment to service provision is needed) are designed to avoid this situation. Taking such an approach appears to be supported by disabled and vulnerable consumers (see PRINCIPLE 2). However, care has to be taken to include needs that are relevant to emergency situations (e.g. ongoing medical access to water) and needs that are required for emergency *and* everyday management or interaction with a service (e.g. communication and interaction needs).

Historically, lists of such support needs, reasonable adjustments, or changes to service have not been widely available. However, projects such as **WhatWeNeed.Support** and Experian’s Support Hub have worked to define these both with consumers and essential service firms and also to make these publicly available as open-source resources (see (BOX 6)³²).

BOX 6

EXAMPLES OF ACTIONABLE SUPPORT NEEDS: EXPERIAN SUPPORT HUB

(www.experian.co.uk/supporthub)

When organisations write to me:

- I cannot reply in writing to letters or post
- Send in a format I can listen to (audio CD)
- Send in Braille Grade 1
- Send in Braille Grade 2
- Send in large print (18-20 point)
- Send in giant print (20-32 point)
- Use a light pastel coloured paper to reduce colour contrast

Speaking to me on the phone:

- I cannot speak on the phone - do not call me
- I use text-to-speech software to communicate - please take this into account
- When calling me use Relay UK
- When I call you I need to use Relay UK - please take this into account
- Where possible, only phone me between 8am to noon
- Where possible, only phone me between noon to 5pm

Meeting me in person

- I cannot attend meetings in person
- I have someone that will accompany me to provide support - please take this into account
- I have an assistance dog that will accompany me - please take this into account
- I prefer to meet or wait in a quiet space (if available)
- I prefer to meet in an open area with people around (if available)
- I will bring my own BSL interpreter with me - please take this into account
- I will bring my own manual deaf-blind interpreter with me - please take this into account
- I need you to arrange for a manual deaf-blind interpreter to be present (if we schedule a meeting)
- I need you to arrange for a BSL interpreter to be present (if we schedule a meeting)
- I require a hearing loop
- I need to see your face when you speak- it helps me to understand
- I find social interaction difficult - please take this into account
- My movement may be affected (including repetitive or noticeable body movements). Please ignore this and do not draw attention
- I require mobility support - please assist me

Notes: We recognise that there may be circumstances (particularly where there are multiple needs or complex situations) when wider cause or condition information may also need to be recorded for practical or regulatory purposes, but this emphasis on 'actionable support needs' is a key one.

Principle 5:

Consumers want to feel in control (even if some decide to never exercise this)

Clearly, one driver for a consumer disclosing and sharing a support need is to receive support and experience a positive change in the way in which their essential services work for them. However, we should not assume that every disabled or vulnerable consumers will want to 'disclose then delegate' all future decisions about how their information is used or shared with other organisations:

i. Autonomy and control are vital to many disabled and vulnerable consumers.

Alongside transparency (see below), having a range of controls over their disclosed information is important for many of these consumers. Clearly, there will be exceptional circumstances where information needs to be shared to prevent or manage serious harm to a consumer. Furthermore, some essential service organisations in a data-sharing network may not want or feel they need to confirm every decision about data sharing or usage with the consumer (citing this as not realistic or legally required under the Data Protection Act 2018). However, organisations taking such an approach **need to be clear when and in what specific circumstances sharing would take place** without the consumer having a role in this choice, and also communicate these broad situations in advance to the consumer (for transparency and clarity). Without taking this step, such actions could both act as barriers to future disclosure or miss scenarios where sharing (without consumer involvement) could lead to harm or detriment. Finally although some consumers may indeed wish to 'disclose and delegate' any future decisions about how their information is used/who it is shared with, this represents a decision or control in itself (and needs to be able to be revoked at any time). **BOX 7** illustrates the importance of this principle.

ii. Transparency is also key - as indicated above, a clear and accessible explanation to consumers of how any disclosed data will be used and shared (including with whom and for what purposes) is essential. These explanations need to be given in written documentation (such as Data Protection Privacy Notices), with accessible formats of these explanations being provided (as disabled and vulnerable consumers may often require this), and with this information being given at the operational point where a consumer makes any decision about their disclosed data being recorded and shared (rather than being only found in wider policy or privacy notice documents).

iii. Third party representation and decision-making also needs consideration - there will be circumstances where a consumer wishes for a known and trusted third-party (such as friends, families, or wider support workers), as well as those with a mandate of authority to act on a person's behalf, or to be involved in making decisions about their data-sharing. This third-party access will need to be factored into the design of any disclosure and data-sharing system, with a particular awareness of the different levels of delegated decision-making that a consumer may wish to give to any third-party.

BOX 7

CONSUMER CONTROL: ACCESS AND REVISION

ACCESS

There will be circumstances where a consumer may want many organisations to know about their support needs or situation. An example of this (taken from the financial services sector), may be a consumer with a gambling addiction who wants every creditor organisation to automatically block their applications for credit (including firms that they are not already a customer of, as well as firms where they are).

However, consumers may more often want to control which organisations see their data (and which do not), or to be given the ability to 'opt-out' of data-sharing if this is not possible. Without such an option, situations may occur where personal or special category data are shared with an organisation that a **consumer did not anticipate or wish to see this**.

For example, take a potentially future scenario where energy firms and Local Authorities are part of an expanded PSR/'Tell Us Once' network, and where this network automatically shares disclosed data about vulnerability/disability among relevant participating organisations.

Here a number of customers in an energy firm's customer base could potentially also be employees of one of these Local Authority organisations, creating a situation where either (a) an employer organisation could receive sensitive information that had not been consciously or otherwise disclosed to them by an employee (which could result in unintended consequences); and/or (b) an awareness of the likelihood of this happening stops individuals from either disclosing their support needs to the original energy firm, or participating in wider data-sharing.

CHANGING

A consumer's support needs or circumstances can change over time. This means that consumers need to be able to revise and revoke their support needs across a selection or all of the essential service organisations participating in a 'Tell Us Once' system.

We are aware, however, of current data-sharing arrangements where:

- an organisation that receives an original consumer disclosure **can** easily share and cascade this information with external health and emergency service organisations in the wider network to better support the customer (meeting the 'Tell Us Once' principle)
- but where the same organisation **cannot** help consumers to revise, update, or remove this information across the wider 'Tell Us Once' network, and where the consumer has to then manually contact every one of the organisations it was shared with.

This underlines the importance of not treating disclosure as a single action - some consumers will need to disclose multiple times to ensure the data that an organisation holds is **accurate, relevant and reflective of their current situation** (as support needs may change over time). Critically, in all of this, it should be transparent to the consumer (and in wider public explanations) how disclosed data will (and will not) be used, and which organisations will have access.

Principle 6:

Consumer data-sharing portals must be accessible (a key test of our values)

As noted earlier, data-sharing relies on data. Given that much (but not all) of this information can come from consumer disclosures, it is important to adopt a strategy that improves and sustains levels of disclosure.

One approach to achieving this is to use a consumer portal. This places consumers at the centre of data-sharing arrangements, allowing them to:

- easily make their initial disclosure
- select which support needs - from a list of options - they would like organisations to meet in both emergency and everyday service use circumstances
- select which organisations - from those participating in the data-sharing network - they want to share support these needs with (and which they do not)
- receive clear explanations of which selected organisations can meet these needs (as not every organisation will be able to meet every support need)
- receive clear explanations of how the selected organisations will use any shared data
- signal their agreement for the data-sharing to take place on the basis of these explanations
- receive updates - via the portal - when an organisation has received/acted-on their need
- revise, update, delete, or revoke any shared information across selected organisations (or receive clear explanations of what is/is not possible).

Such a consumer portal approach puts the consumer in control of their data. It also ensures transparency (as the consumer is aware at all times of who has access/use of these data), as well allowing consumer support needs to remain accurate and up-to-date.

Clearly any portal for disabled or vulnerable consumers requires an accessible design that reflects the needs of those using it). It would be damaging if a portal for consumers to share their need for extra support was designed in an inaccessible or exclusionary way. This includes any charges being made by such portals to a consumer to share and manage their support needs with multiple organisations. It also covers situations where 'Plain English' or 'Plain Numbers' approaches were not used to simplify and present information to consumers. Equally, while such a portal is likely provided via a self-serve digital channel, it would be an oversight not to work towards disclosure or management by other channels (e.g. email or non-digital channels such as post or telephone), or to delegate this activity to an authorised third-party.

Finally, disabled and vulnerable consumers are often best placed to know what support they need (either in an emergency or for everyday account tasks). **However, this is not the same as an individual knowing what support a specific organisation could provide to them, or understanding the benefits or difference that such support could make to their lives.** Consequently, consumer portals need to offer a clear explanation of what support is on offer, how this support would work in practice, what difference the support could make, and how quickly that support would be enacted.

Principle 7:

Consumer data-sharing portals should lead to support (accessible and timely)

Clearly, when a consumer shares a need for support (which an organisation receiving this data has indicated it can meet), this should lead to that support and help being given. This might not always be immediate (e.g. a support need may be relevant only in an emergency situation). However, it is critical that in meeting one specific support need, organisations also take account of the other support needs that a consumer has disclosed. For example, there is no benefit in an organisation giving advance notice of an interruption to supply to a consumer, if that communication is not in the accessible format the consumer requires. Or if an organisation delivers essential items to a consumer during an emergency situation, but leaves these items where a disabled consumer cannot reach them.

As well as being accessible and timely, data-sharing arrangements also need to be well-designed.

With this in mind, research undertaken by Citizens Advice compared three different types of ‘Tell Us Once’ systems currently available to consumers (**BOX 8**). Using a criteria that overlaps with many of the principles in this paper, Citizens Advice found that only one of these systems (in the far right-hand column) best aligned with Citizen Advice’s ‘blueprint’ for an ideal customer data-sharing journey, and recommended that Government leadership was needed to achieve a cross-sector solution³³.

BOX 8

‘Tell us Once’ systems: Citizen Advice comparative review of existing consumer portals

Where are we now?

Recent years have seen new products and services emerge for firms to help them improve the identification of and support provided to their customers. The examples below show how these products compare to the ideal customer journey.

High-level vulnerability flags

There are organisations that work to provide a central, independent register of vulnerable people that can be accessed by service providers.

- ✗ Available to use by all consumers across all essential services
- ✓ Highlights additional care is needed when interacting with consumers
- ✗ Consumer can view support available to them
- ✗ Single disclosure of needs can be shared with multiple service providers
- ✗ Consumer controls which firms can see their data
- ✗ Consumer can easily update their information if their circumstances change

Connecting services to consumers

There are organisations that offer tools for assessing the vulnerability of customers so service providers can offer them appropriate products and services

- ✗ Available to use by all consumers across all essential services
- ✓ Highlights additional care is needed when interacting with consumers
- ✓ Consumer, or the agent supporting them, can view support available to them
- ✗ Single disclosure of needs can be shared with multiple service providers
- ✗ Consumer controls which firms can see their data
- ✗ Consumer can easily update their information if their circumstances change

Disclosure portal for support needs

Consumer-facing platforms exist that allow consumers to share their support needs with multiple organisations at the same time.

- ✗ Available to use by all consumers across all essential services
- ✓ Highlights additional care is needed when interacting with consumers
- ✓ Consumer, or the agent supporting them, can view support available to them
- ✓ Single disclosure of needs can be shared with multiple service providers
- ✓ Consumer controls which firms can see their data
- ✓ Consumer can easily update their information if their circumstances change

Firms choose whether or not to invest in these services, resulting in a patchwork of different experiences for consumers. There is still no solution which meets every stage of the consumer journey.

Government leadership is needed to achieve a cross sector solution.

‘Tell us once systems’: Citizen’s Advice Review Notes: Citizens Advice did not name the Tell Us Once systems they reviewed. In future reviews it would be useful to know how current organisations and platforms compare in order for consumers to make an informed choice.

Principle 8:

Organisations will use shared data differently (transparency is therefore vital)

While ‘improving support to consumers’ may be a common objective across those organisations participating in a data-sharing network, in practice each organisation will want to use any shared vulnerability data in different ways and to take different actions.

At the outset of any Tell Us Once or data-sharing network, it is likely that the types of participating organisations will come from a limited range of sectors (e.g. water, energy, telecoms, financial services). Consequently, this may not cause significant difficulties in explaining to consumers how their data may be used (as consumers may reasonably expect, and able to understand, this).

However, it is important to recognise that data-sharing networks and their participants are not set in stone - they will need to evolve, change, and improve over time to meet the different support needs and situations that disabled and vulnerable customers will face.

Critically, this includes the fact that new organisations - perhaps not originally included in earlier stages of the ‘Tell Us Once’ system’s evolution - may join the ‘network’, while existing organisational members in the data-sharing system may wish to expand their remit and involvement. In such situations, it:

- may not be as immediately obvious to consumers how their data might be used by these new organisations from other sectors or backgrounds
- needs to be carefully defined and explained how these new organisations might also wish to ‘onward share’ this information with their own partners (see example in **BOX 9**).

Consequently, as each organisation and sector joins a data-sharing network, a need exists for these organisations to (i) publicly commit to only using the shared data for the purposes of clearly defined and agreed types of support, (ii) that this usage is monitored over time (by a central body), and (iii) it is made clear to consumers what these purposes are, and what controls they have over this data-sharing and processing.

BOX 9

NEVER SET IN STONE: NEW ORGANISATIONS, NEW SECTORS, NEW IMPACTS

Consider a situation where Local Authorities join an existing, up-and-running, and successful data-sharing network that (until this point) has only included energy and water organisations. Here the inclusion of Local Authorities brings many potential advantages (in terms of everyday service delivery), but Local Authorities are large organisations that incorporate many different departments. Consequently, it could be perceived or realised that disclosed consumer data is then shared with departments such as Adult/Child Social Services or Council Tax collection. If explanations or controls over data-sharing are not adequate, consumers may perceive these additions as risky or harmful, and potentially could prompt withdrawals from the wider network arrangement, or deter disclosure in the first place.

Principle 9:

Organisations in a 'sharing network' do not need the same lawful base to share

In any data-sharing, careful attention needs to be paid to the Data Protection Act (2018). This guide cannot cover the entirety of data protection legislation (for this, see the ICO's own website or data-sharing code, or Fitch et al 2020 Vulnerability, GDPR and disclosure). However, it is important to make one key observation: **different organisations in a 'sharing network' do not need to use the same lawful processing base to share information.**

Currently, some data-sharing arrangements are aiming to operate with organisations who all use the same Article 9 lawful base for processing special category data (most notably Substantial Public Interest (SPI) or Explicit Consent (EC) base), on top of the required Article 6 base.

However, as data-sharing networks are planned and developed, it often becomes apparent that potential organisational participants are going to use a mixture of different lawful processing bases (again some will be using SPI, others will be employing EC, and this may reflect a wider tradition or approach in that industry or sector).

While some commentators may contend that every organisation participating in a data-sharing arrangement could move to the same lawful processing base, this is practically unrealistic. This may be due to some firms or sectors - as well as their consumer base - favouring a particular lawful processing base or tradition, or resource limitations (in terms of the time and costs to move multiple firms to the same processing approach). Consequently, requiring all organisation to use the same lawful processing base could deter or slow the development of data-sharing networks (as it could act a barrier to engagement).

However, after consultation with the Information Commissioner's Office about this (December 2023²⁵), the following has been made clear to us:

- individual organisations are not usually permitted to swap from one lawful processing base to another (e.g. a customer refuses an approach from an individual organisation for EC to process their data, so the organisation decides to use SPI - this is not permitted)
- **but there is nothing in the DPA 2018 and legislation** that says different organisations in a data-sharing situation have to rely on the same lawful processing basis.
- Instead, before sharing information, organisations must:
 - consider their compliance with DPA legislation (including fairness and transparency)
 - be mindful not to set unfair consumer expectations - in particular, the 'sharing' organisation needs to explain they are relying on, for example, Explicit Consent only to share the information concerned, and that once this is shared the 'receiving' organisation will be processing this using a different lawful base in order to provide the support need that has been disclosed (which could be achieved via clear explanation at the point of disclosure)
 - explain that if there were any consumer concerns about how their data were used by a 'receiving' organisation, then contact and dialogue would normally be with that receiving organisation (rather than the 'sharing' organisation)
 - not only set up a data-sharing process but consider it good practice to have a written data-sharing agreement which explains the process itself, the benefits of this, the different processing bases used by different organisations, and other pieces of information required by data protection law.

In short, in situations where there is a 'sharing organisation or central hub' and 'receiving organisations' the ICO advice is that it is legally allowed for participating organisations in a 'Tell Us Once' system to use different lawful processing bases.

Principle 10:

Meet current need, but watch for future harm (avoid unintended consequences)

Current need: the defining test

The **defining test** of any vulnerability data-sharing scheme is not found in metrics relating to disclosure levels, volume of shared data, or the number of registered consumers or participating organisations in a sharing network (as important as these indicators are).

Instead, the key measure of vulnerability data-sharing is **whether a consumer receives the support they need** in an emergency situation or everyday circumstance. Achieving this involves ensuring that consumer disclosure leads to organisational action - without taking this step, we are left with data but no delivery.

Future harm: watching the horizon

Any initiative involving data need to consider not only its immediate and intended purpose, but also the **potential future uses** of this data. Importantly, this includes the potential and perceived risks to disabled and vulnerable consumers of this future use.

There is already a literature on how health data within certain essential service sectors are used to - it is argued - calculate and increase cost for people with health problems³⁶. Further, there have been concerns raised and campaigns against research studies in the wider scientific community where it has been argued that the data collected for one purpose could be used in different and potentially harmful ways in the future .

The key point to take from this, is that any data-sharing or Tell Us Once network must routinely monitor and consider any future and inadvertent harm that might be encountered and take steps to remedy this. Failure to do this from the outset will cause ongoing problems of trust, impact, and engagement. Consequently, the principle of transparency needs to extend here to a clear statement of how such future uses of data will be monitored and controlled (e.g. in the context of training AI models), and how consumers will be informed about potential new uses.

D. Deciding: how do we take the opportunity?

This paper has examined vulnerability, disability, and data-sharing across the essential service sectors. It has offered **10 principles** to help make it simpler, fairer, and more transparent:

- for vulnerable or disabled consumers to disclose and share their circumstances and support needs with multiple organisations through one simple process
- for essential service organisations to transparently share information about consumer circumstances and needs between themselves and other relevant bodies
- to use such data-sharing to prevent and minimise harm, disadvantage, loss, or exclusion among these consumers in emergency situations and everyday service use.

Importantly, these **10 principles** encourage everyone involved in the design, development, and delivery of Tell Us Once and data-sharing approaches to not only focus on the technical and operational challenges ahead of us, but to embed the **human use-case and need** for a better disclosure and data-sharing scheme to improve the lives of millions of consumers.

In the current policy, political, and practical context, we have in our hands a ‘once in 25 years opportunity’ to make this happen – and this chance needs to not only be taken decisively, but through a collaboration between vulnerable and disabled consumers, essential services, regulators and other key actors based on a recognition that:

1. speak the same language (define our key terms)
2. data-sharing needs data (so avoid the known barriers to consumer disclosure)
3. this is not a technical project (keep the focus on solving the human problem)
4. ‘actionable support needs’ are the key (rather than higher-level flags alone)
5. consumers want to feel in control (even if some decide to never exercise this)
6. consumer data-sharing portals must be accessible (a key test of our values)
7. consumer data-sharing portals should lead to support (accessible and timely)
8. organisations will use shared data differently (transparency is therefore vital)
9. organisations in a sharing network don’t need the same lawful base to share
10. meet current need, watch for future harm (avoid unintended consequences)

Author biographies

This paper was written by Chris Fitch, Christine Tate, Dan Holloway, Elizabeth Blakelock, Faith Reynolds, Jo Giles, Johnny Timpson, Kevin Still, Lee Healey, Shani Dhanda, Steve Crabb, and Vanessa Northam.

This group have all been involved in work on data-sharing, vulnerability, and disability over the last decade, and have each contributed to this paper in an independent capacity.

Full author biographies and conflict of interest statements are found below. The views of the authors are their own and do not represent those of the organisations with which they work.

Dr Christopher Fitch is Vulnerability Lead at the Money Advice Trust, a Research Fellow at the Personal Finance Research Centre (University of Bristol), and a Fellow of the Royal Society for Public Health. Since 2007, he has led a programme of guidance, research, training, and intervention on vulnerability across the essential services sectors.

Register of interest: Chris advises the Experian Support Hub project in a paid capacity.

Christine Tate (MBA) is Managing Director of Partnerships for Good Ltd. Christine provides a consultancy service to charities and private organisations, developing partnerships to support disadvantaged and marginalised consumers. She has had a career in key senior management positions in leading utility companies. Christine has living experience of primary lymphoedema.

Register of interest: nil.

Dan Holloway is Co-convenor of the Futures Thinking Network at The Oxford Research Centre for the Humanities, and researches and writes about disability, technology, and inclusion. He is CEO of the University of Oxford spinout Rogue Interrobang. Dan has lived experience of bipolar disorder and a selection of neurodivergences.

Register of interest: Dan advises the Experian Support Hub project in a paid capacity.

Dr Elizabeth Blakelock is an inclusion specialist. Drawing on both her academic work (a feminist critique of essential service regulator decision making) and her lived experience of disability and neurodivergence, Dr Blakelock delivers practical change to provide accessible essential services.

Register of interest: nil.

Faith Reynolds works in an advisory capacity across a range of fintech, Smart Data and Open Finance initiatives. She has been a leader in developing Open Banking and Smart Data in the UK, is an advisor to the board at TISA, and is also leading on research initiatives to improve communications and break down barriers to investing.

Register of interest: Faith works with start-up Amplified Global, is Chair of the Advisory Board for UKFin+, and is a non-executive director at Fair4All Finance.

Jo Giles is a specialist in achieving change on vulnerability and accessibility in essential services. A member of the National Mental Capacity Forum, she works to build better ways to respond, reduce, and prevent vulnerable situations, and achieve equal access for consumers.

Register of interest: nil.

Johnny Timpson OBE has lived experience of disability and is a Financial Inclusion Commissioner and a member of both the Building Resilient Households Group and GAIN (the Group for Autism, Insurance, Investment and Neurodiversity).

Register of interest: Johnny holds roles with the University of Edinburgh Business School Supporting Healthy Ageing at Work (SHAW) Project, Surviving Economic Abuse Charity, Vocational Rehabilitation Association UK and the GriefChat Counselling Service.

Kevin Still is a director of trade body DEMSA, a NED for the Vulnerability Registration Service (VRS), on the MaPS SFS governance group and part of the HM Treasury Fairness Group, including the vulnerability and affordability sub-groups.

Register of interest: these roles are undertaken on a voluntary and unpaid basis.

Lee Healey is the founder and CEO of IncomeMax, a social enterprise helping families in the UK to maximise their income and take control of their finances. Lee is also an advisory board member for the Money and Mental Health charity, a MALG ambassador, and a stakeholder representative for the Energy UK Vulnerability Commitment Advisory Board.

Register of interest: IncomeMax is funded through partnerships where there is a specific interest in supporting vulnerable people.

Dr Shani Dhanda is a Multi-Award-Winning Disability Inclusion & Accessibility Consultant, Broadcaster & Social Entrepreneur, and has been identified as the most Influential Disabled Person in the UK, by the Shaw Trust.

Register of interest: nil.

Steve Crabb is an independent chair and non-executive director specialising in improving the experience of customers in the utility sector in general, and those with additional service needs in particular.

Register of interest: Steve advises the Experian Support Hub project in a paid capacity, and has also been paid for advice for PSR data sharing by water industry body Water UK.

Vanessa Northam is Head of Charity Development at StepChange and a recognised strategic leader on consumer vulnerability in the financial services, energy, fintech, and charity sectors. Prior to StepChange, Vanessa worked in an Open Banking start-up and in leading E.ON's vulnerable consumer strategy.

Register of interest: nil.

The series represents best practice guidance but does not constitute legal or regulatory advice.

Permission to share: This document is published under a Creative Commons licence:

Attribution-NonCommercialNoDerivs 3.0 Unported (CC BY-NC-ND 3.0) England and Wales

Licence. <https://creativecommons.org/licenses/by-nc-nd/3.0/>

Appendix 1 – vulnerability definitions

FINANCIAL CONDUCT AUTHORITY

“A vulnerable customer is someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care”¹⁹

OFGEM

“[A consumer is vulnerable] when [their] personal circumstances and characteristics combine with aspects of the [energy] market to create situations where [they] are: significantly less able than a typical consumer to protect or represent [their] interests; significantly more likely than a [domestic] consumer to suffer detriment or that detriment is likely to be more substantial”¹²

OFCOM

“Anybody can face circumstances that lead to them becoming vulnerable - temporarily or permanently. This might include physical or mental health problems, specific characteristics such as age or literacy skills, or changes in personal circumstances such as bereavement, job loss or changes in household income. [We] refer to people whose circumstances have led them to becoming vulnerable as ‘vulnerable customers’. We recognise that organisations use a range of different terminology and some people might not like to be labelled as a vulnerable customer”¹⁶

OFWAT

“A customer who due to personal characteristics, their overall life situation or due to broader market and economic factors, is not having reasonable opportunity to access and receive an inclusive service which may have a detrimental impact on their health, wellbeing or finances”¹⁵

ICO

“Individuals can be vulnerable where circumstances may restrict their ability to freely consent or object to the processing of their personal data, or to understand its implications. Most obviously, children are regarded as vulnerable to the processing of their personal data since they may be less able to understand how their data is being used, anticipate how this might affect them, and protect themselves against any unwanted consequences. This can also be true of other vulnerable sections of the population such as elderly people, or those with certain disabilities. Even if the individuals are not part of a group you might automatically consider vulnerable, an imbalance of power in their relationship with you can cause vulnerability for data protection purposes if they believe that they will be disadvantaged if the processing doesn't go ahead.”

References

- ¹Department for Work and Pensions (2023). Family Resources Survey 2021 to 2022. [adult = individuals 15 to 80 and over]
- ²Financial Conduct Authority (2023). Financial Lives Survey 2022.
- ³Carers UK and Centre for Care, Sheffield University (2022). Cycles of caring: transitions in and out of unpaid care.
- ⁴Business Disability Forum (2021). What disabled consumers choose to buy and why.
- ⁵Financial Conduct Authority (2023). Financial Lives Survey 2022.
- ⁶Money and Mental Health Policy Institute (2021) The State We're in.
- ⁷Money and Mental Health Policy Institute (2016) In Control.
- ⁸Money and Mental Health Policy Institute (2018) Access essentials.
- ⁹Money and Mental Health Policy Institute (2023). Too much information? Key considerations for vulnerability data-sharing.
- ¹⁰Utility Regulator NI (2023). <https://www.uregni.gov.uk/consultations/best-practice-framework-consultation-proposals-code-practice-consumers-vulnerable>
- ¹¹This box has been constructed with the assistance of, and through communication with, Ofgem, Ofwat, Consumer Council for Water.
- ¹²Ofgem. (2019). Consumer vulnerability strategy 2025.
- ¹³Brealey J. (2023). Speech to Ofgem's Vulnerability Strategy. <https://www.ofgem.gov.uk/news-and-views/blog/jonathan-breareleys-speech-ofgems-vulnerability-summit>
- ¹⁴Ofwat (2016). Practitioners' pack for water companies.
- ¹⁵Ofwat (2023). Service for all – Ofwat's final vulnerability guidance for water companies supporting customers who need extra help.
- ¹⁶Ofcom (2022). Treating vulnerable customers fairly. A guide for phone, broadband and pay-TV providers. Updated.
- ¹⁷Ofcom (2022). 2022 Review of Postal Regulation. Statement.
- ¹⁸Ofcom (2023). General Conditions of Entitlement. Unofficial Consolidated Version.
- ¹⁹FCA (2021). Finalised guidance. FG21/3. Guidance for firms on the fair treatment of vulnerable customers.
- ²⁰ICO (2022). Data Sharing Code of Practice.
- ²¹ICO (2022). ICO25 - empowering you through information.
- ²²Department for Business and Trade (2023). Smarter Regulation: Strengthening the economic regulation of the energy, water and telecoms sectors. As regulated by Ofgem, Ofwat and Ofcom.
- ²³Data Protection and Digital Information Bill (2023). <https://bills.parliament.uk/bills/3430/publications>
- ²⁴Digital Economy Act (2017). <https://www.legislation.gov.uk/ukpga/2017/30/contents>
- ²⁵UK Government (2018) Code of Practice for public authorities disclosing information under Chapters 1, 3 and 4 (Public Service Delivery, Debt and Fraud) of Part 5 of the Digital Economy Act 2017.
- ²⁶Money and Mental Health Policy Institute (2021) The State We're In
- ²⁷Mind (2011) Still In the Red: Debt and Mental Health.
- ²⁸Mind (2008) In the Red: Debt and Mental Health.
- ²⁹Money and Mental Health Policy Institute (2023) Too much information? Key considerations for vulnerability data-sharing

³⁰See for e.g. Fitch C, Holloway D, D'Arcy C (2022) Recording Disclosure. Money Advice Trust and MMHPI.

³¹Fitch C, Holloway D, D'arcy C (2022) Disclosure Environments. Money Advice Trust and MMHPI.

³²See the website (full URL as follows): [WhatWeNeed.Support](https://www.whatweneed.support)

³³Citizens Advice (2023) Closing the Gap: How to improve customer support in essential services.

³⁴Fitch C, Bell R, Trend C. (2020) Vulnerability, GDPR and disclosure. Money Advice Trust/MALG.

³⁵Personal Correspondence from ICO (2023) [available on request from author].

³⁶Financial Conduct Authority (2020). Signposting to travel insurance for consumers with medical conditions. PS20/3.

³⁷<https://liamodell.com/2023/09/28/spectrum-10k-consultation-autism-research-dna-hopkins-van-mil-transcripts-webinar-university-of-cambridge-simon-baron-cohen>

³⁸ICO (2024). <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when11>

The paper represents guidance but does not constitute legal or regulatory advice. Permission to share: This document is published under a Creative Commons licence: Attribution-NonCommercialNoDerivs 3.0 Unported (CC BY-NC-ND 3.0) England and Wales Licence.
<https://creativecommons.org/licenses/by-nc-nd/3.0/>