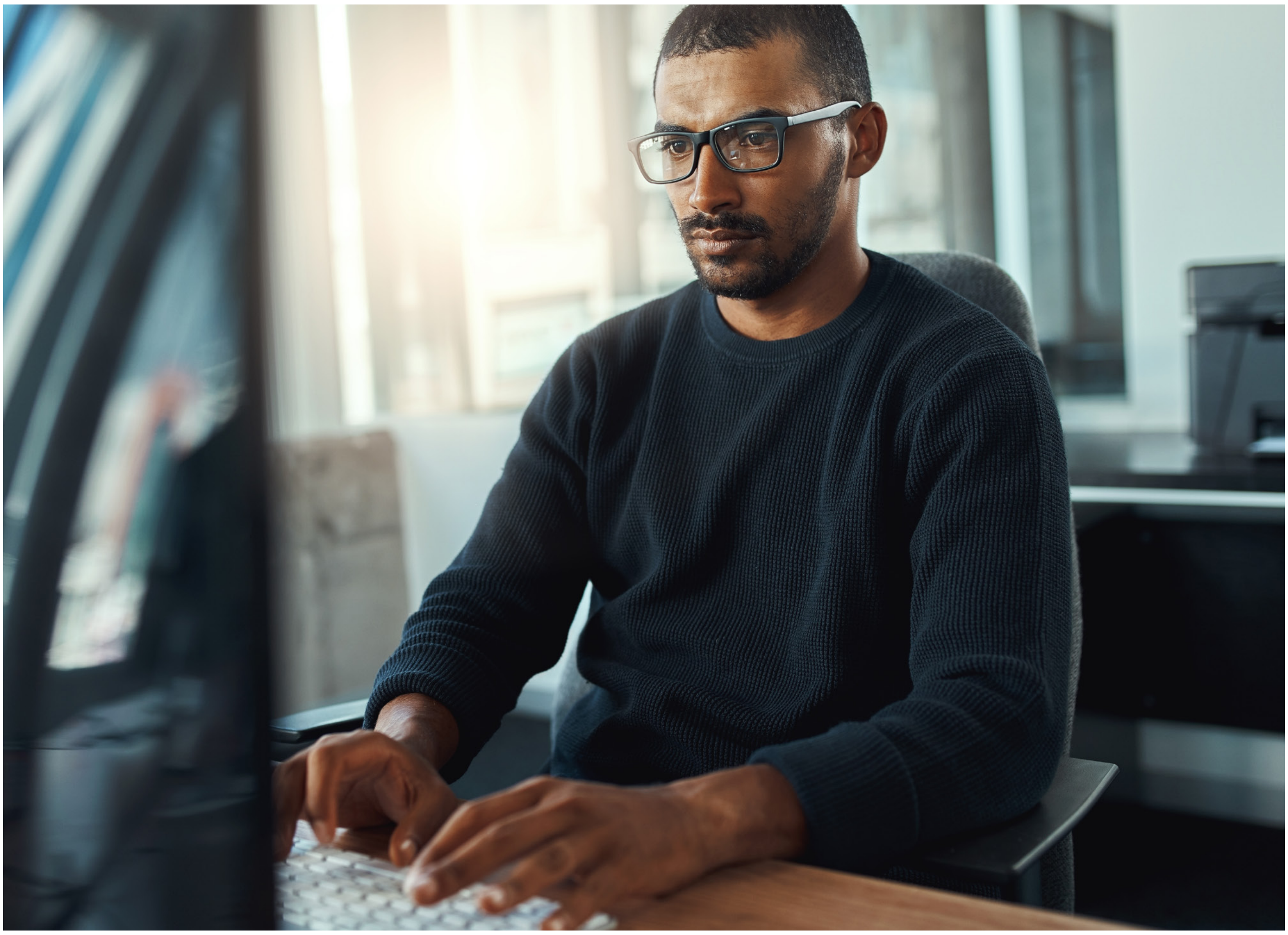
RECORDING DISCLOSURE

Processing data from consumer mental health disclosures



Guide three in a series on mental health disclosure

Chris Fitch, Dan Holloway and Conor D'Arcy

November 2022

Contents

Introduction

About the authors

Chris Fitch is Vulnerability Lead at the Money Advice Trust and a Research Fellow at the Personal Finance Research Centre, University of Bristol.

Dan Holloway is a disability activist, Co-convenor the Futures Thinking Network at The Oxford Research Centre for the Humanities, CEO and founder of Rogue Interrobang, a spin-out of the University of Oxford.

Conor D'Arcy is Head of Research and Policy at Money and Mental Health.

Introduction

Being a consumer with a mental health problem can be difficult.

This is because everyday services and companies – like banks, energy suppliers, or mobile providers – don't always understand the needs that people with mental health problems can have (which can span challenges from communication, interaction, decision-making, to concentration).

This means getting what you need from these everyday services can be much, much harder. It means using up energy, effort, and time trying to get these essential services working for you.

And it means lives that could have been spent *living*, become an everyday grind of just getting by.

Disclosure

For some time, disclosure has been seen as one way to break this grind. This is based on the logic that if consumers simply told firms about their mental health problems, then organisations would have the information needed to deliver relevant help and support.

And – as seen in Guide One – regulators expect firms to encourage and act on such disclosures.

However, such reasoning can fall short where it:

1. **makes the consumer solely responsible for disclosure** (rather than firms also taking responsibility for encouraging and acting on disclosure)
2. **overlooks the fact that most consumers with mental health problems do not disclose** (due to unaddressed practical barriers or perceptions of negative consequences)
3. **distracts from the actions a firm should take once a disclosure has been made to them** (including how staff should initially manage these, and 'how far' firms should go with support)
4. **frames disclosure more as a technical process rather than a human interaction** (where upset, frustrated and scared consumers disclose in hope of positive change)
5. **under-considers how the 'data-footprint' left behind by disclosure will then be used** (including whether firms or consumers should control how this data can be used)
6. **sees disclosure in isolation – rather than as part of a wider strategy of linked actions** (where disclosure sits alongside journey design, identification, and support options).

Consequently, while disclosure represents a well-known and widely adopted strategy among firms, little consideration has been given to what actually 'works' to underpin such a strategy.

Three guides

For these reasons, Money and Mental Health and the Money Advice Trust have collaborated on three disclosure guides, informed by evidence summaries and new research.

- **Guide One is about disclosure environments**. Outlining the fundamentals of disclosure, this explains how firms can encourage consumer disclosure of mental health problems.

- **Guide Two is about responding to disclosures once they are made.** This describes what makes for a 'successful disclosure' in technical and human terms.

- **Guide Three is about data.** This covers the encoding of disclosure into data to help consumers. It also considers the balance between firms wanting to record data to protect consumers from future harm, against consumers' controlling and consumers wanting to control what is recorded about them.

Section one

UNDERSTANDING DISCLOSURE

Establish your reasons

Every firm should know its **reason for recording data** from a consumer's mental health disclosure.

This is because when a consumer:

- makes contact to tell us something (e.g. a request, update, support need)
- discloses a problem they are having (whether product-related or not)
- explains the cause of that problem (financial, health, life event, or other)

staff must:

- know what data to record, why this needs recording, and how it will be used
- be able to explain this clearly to consumers to ensure transparency and fairness
- and allow the consumer – where possible – to consent or object to this use of their data.

This requires balancing data protection, staff practice and consumer viewpoints.

Data protection

The Information Commissioner's Office (ICO) is the UK's data protection regulator.

The ICO requires firms to state what data they want to record, why it is necessary to do this, and to explain to consumers how this will be done legally, fairly and transparently.

This guide covers two approaches (explicit consent and substantial public interest) that firms can choose to employ when recording or processing disclosed health data.

Each of these approaches (known as 'lawful bases') gives consumers a different type of control or say over whether a firm can record and retain their disclosed information.

This guide aims to give firms insight into what consumers think of these approaches – a viewpoint that is often not available when firms decide on which processing base to employ.

However, other lawful bases are available and we make reference to further guidance on these.

This guide

To help firms understand disclosure from a consumer perspective, this guide presents new data from interviews with consumers with mental health problems about their views on different processing options (and the 'say', control, and choices they want over what is recorded).

Live up to GDPR principles and rights

The ICO requires all firms to have a legal basis on which to process consumer data.

On page 10, we focus on two lawful bases that firms often consider for processing health data. But we start here with a re-cap of key definitions, GDPR principles, and individual rights.

Key definitions

Knowing the following is central to understanding the lawful bases for processing:[1]

- **Data processing** is almost anything that is done with data including collecting, recording, storing, using, analysing, combining, anonymising, sharing, or deleting information.
- **Personal data** is information about a living individual – this includes things like a person's name, address or birth date. It can also cover information about a person's interactions or transactions with firms, including online interaction.
- **Special category data** involves sensitive data in need of greater protection. There are nine types including health data (which covers direct and indirect references such as where a support need – like access to a hearing loop – could infer a consumer's health condition).
- **Health data** includes the past, present, or future physical or mental health of an individual, including injury, disease, disability, disease risk, health care provision or diagnosis.

For more detail on this (and other data protection issues) see the ICO website and the Money Advice Trust and Money Advice Liaison Group's 'Vulnerability, GDPR, and Disclosure' guide.[2]

Principles for processing

There are seven principles firms must follow in processing data under the UK GDPR (Figure 1).[3]

These are equally important. However, as our consumer interviews show later, concerns about fairness and transparency ('how will my data be used – do I have a choice?') were prominent.

This is vital. While consumers may expect firms to collect data about their financial situation, they may reasonably not always anticipate data about their health or life circumstances to be recorded. From the outset, transparency about how firms will process such consumer data is therefore key.

Individual rights

There are eight individual GDPR rights – these do not apply all the time but are 'switched on' (or off) depending on the lawful processing base a firm has adopted (see Figure 1). Those familiar with data protection may know about these, but it should not be assumed consumers will. Firms need to always take this into account and ensure consumers are fully aware of their rights, know what their options are, and are able – through a firms' actions – to trust them with their data.

Figure 1: The seven GDPR principles

1 **Lawfulness, fairness, transparency**	**Crystal-clear, fair, legal** Firms need to remember that consumers making mental health disclosures may be vulnerable to harm or difficulty. Firms may need to make adjustments to standard practice like alternative format information, more detailed explanation, and reminders of key rights.
2 **Purpose limitation**	**Consumers have fears** Consumers may worry about how their mental health data will be used. Without reassurance, they can fear data being given for one purpose, but being used later for a different and unwanted purpose (e.g. to decide on a credit application).
3 **Data minimisation**	**Minimal ≠ No data** Consumers will not want to disclose their situation repeatedly. Firms need to capture what a consumer is vulnerable to, the type of support that might help, and any other contextual information to prevent, minimise, or avoid harm.
4 **Accuracy**	**Health changes** Time can play a key role in consumer vulnerability. Some consumers will be ‘temporarily vulnerable’, others will experience ‘fluctuating vulnerability’, many will have ‘long-term vulnerability’, while some will live with a mix of all of the above.
5 **Storage limitation**	**Deletion** Data on mental health that is collected, will also (at some point) need to be removed from a firm’s databases and systems. Firms need to ensure that they have a system that can both identify and delete such data on consumer vulnerability.
6 **Integrity and confidentiality**	**Who needs to know?** Firms need to think carefully about the flags, account notes, and support codes they use to categorise vulnerability. They also need to establish who has access to particularly sensitive information.
7 **Accountability**	**Records and evidence** Mental health data will – from time to time – need judgements to be made on how best to handle or process this information. Firms need to evidence these judgements, so a consistent record of action exists.

Figure 2: The eight GDPR rights for individuals

Right to be informed

About data processing

This means explaining – in firms' privacy information – purpose for processing, data retention periods and any data sharing. Firms should do this at the point of collecting data from a consumer (except where person already has information, or it would involve disproportionate effort).

Right of access

To data held about them

Individuals have the right to access their personal data ('subject access' requests). This request can be verbal or in writing. Firms should respond without undue delay, within one month, and cannot normally charge a fee for this.

Right of rectification

Correct inaccurate data

Reflecting the principle of accuracy, a right exists for inaccurate or incomplete personal data to be corrected. Requests can be written or verbal, and firms should respond without delay within a month (although in some situations, firms can refuse requests).

Right of erasure

Delete my data

Individuals also have the right for their personal data to be erased (the 'right to be forgotten'). Verbal or written requests can be made, and firms have a month to respond. This right, however, only applies in certain circumstances.

Right to restrict processing

Stop processing my data

Individuals can request firms restrict the processing of their data – this means firms can store the data, but not use it. This only applies in certain situations, can be requested verbally or in writing, and firms have a month to respond.

Right to object

Object (unless over-ridden)

Firms must tell consumers about the right. Consumers can object verbally or in writing (with one month for a firm to respond). Exemptions allow the right to object to be 'over-ridden' if a firm has a compelling reason. An absolute right to stop data being used for direct marketing does exist.

Right to data portability

Move my data

This right allows consumers to obtain and reuse their personal data for their own purposes across different services. Consumers can request their personal data is moved, copied, or transferred from one IT environment to another.

Right over automatic processing

Information or human

A right exists about decisions made without human intervention (including profiling of personal data to evaluate and infer things about an individual). Protections include information about the automatic processing being given, and the option to request human intervention or challenge a decision.

Note: these rights do not apply to all lawful processing bases at all times. For a full description see: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Consider consumers in your choice of bases

There are a range of lawful bases that firms can use to process consumer data (see Figure 3).

Firms need to remember that to process:

- 'personal data', firms need one lawful basis from a list in the UK GDPR called 'Article 6'[4]
- 'special category data', firms need two bases: one from Article 6 and one from 'Article 9'.[5]

This section describes two popular bases for special category data (which includes health data). These need to be accompanied by an Article 6 basis. Given its frequent use for this (including its twinning with substantial public interest), this section also outlines the 'legitimate interests' basis.

Lawful base: explicit consent

Seeking explicit consent to process mental health disclosures is probably the best known lawful basis among firms (and in our research, the most expected action by consumers). It involves:

- clearly telling consumers how their disclosed information will be used
- allowing consumers to decide whether to let you use their data in this way
- asking consumers to clearly confirm whether they will let you do this
- reminding consumers that they can withdraw their consent at any time.

To achieve this, firms must firstly meet the basic standards of valid consent as defined by Article 6 (with consent being freely given, obviously made, specific, and withdrawable at any time).[3] They also need consumers to confirm – via oral, written or 'tickable' statements – they agree to a firm's terms for processing data (and that this has been clearly explained to them).[4]

Explicit consent: considering consumers

Some firms worry that consumers may refuse to give explicit consent for their data to be recorded, and that this 'missing insight' could stop them preventing future harm to a consumer. However, before considering processing bases other than explicit consent, firms should note six factors:

1. whether they know the volume of explicit consent refusals that are occurring in practice (concerns within firms about refusal can be greater than the actual number of refusals taking place)
2. whether there is a reason why refusals are taking place (as this can be due to the way in which explicit consent is being sought or explained by staff)
3. whether there is information that can be recorded after a refusal that could be helpful (e.g. recording the support need itself – if this doesn't infer a health condition – or setting a general flag indicating support may be needed at future contact)

4. that other processing bases – as we shall see in the next section – can require firms to clearly demonstrate why explicit consent could not be used, and may require firms to still offer consumers the right to object to their disclosed data being processed
5. that where a consumer refuses explicit consent, a firm cannot turn to a second different lawful base to continue processing disclosed data (this would not be fair, transparent, or lawful)
6. that the fundamental strength of explicit consent is about giving consumers control over how their data is used and processed – adopting other processing options may diminish this.

Lawful base: substantial public interest

With the introduction of the DPA 2018, an option has emerged for firms – the 'economic wellbeing' condition – to process a consumer's disclosed health data *without* their explicit consent. One of 23 'substantial public interest' bases in Article 9,[4] firms can proceed where consumers are:

- aged 18 or over
- at economic risk
- cannot protect their economic wellbeing
- due to reasons of physical or mental injury, illness, or disability.

Under this basis, health data can be processed without explicit consent for any of the following:

- the individual cannot give consent (e.g. where a consumer cannot give consent due to an underlying health condition such as dementia)
- the firm cannot obtain consent (e.g. a health condition disclosure is made via webchat, but a consumer 'disconnects and disappears', and cannot be reasonably re-contacted)
- getting consent would prejudice the ability of a firm to put measures in place to protect a consumer's economic wellbeing (e.g. a consumer disclosing a gambling addiction might refuse consent for this to be recorded, and the absence of this information could lead to the consumer being offered credit that would not otherwise be approved).

Figure 3 Lawful bases for the process of consumer data

Article 6 Lawful Bases	Summary
Consent	Where a consumer gives consent (or someone authorised for them does) which is **freely given**, **obvious** (a positive action to 'opt-in'), **specific** (in terms of the processing purpose), and the consumer knows it can be **withdrawn** at any time. Valid consent is not the same as explicit consent – however, explicit consent does contain all of the above features.
Contract	Where processing data is necessary to deliver a contract (or enter into a contract – e.g. the provision of a quote).
Legal obligation	Processing is required to comply with law or regulation (which law/regulation should be in a firm's privacy information).
Vital interests	Processing needed to protect life (consumer and others). Can be used for special category data in certain situations.
Public task	Processing is necessary to perform a public task, or official duty (this mainly applies to public authorities, although some private water company tasks fall under it).
Legitimate interests	Processing is needed to pursue interests of a firm, third-party, or wider society without over-riding the rights and freedoms of consumers.

Article 9 Lawful Bases	Summary
Substanital public interest	23 conditions in UK law allow firms to process special category data for reasons of substantial public interest. Of these, the safeguarding of the economic wellbeing of certain individuals (Paragraph 19) may in certain circumstances provide an alternative to explicit consent.
Explicit consent	To obtain 'explicit consent' a firm needs to: **first**, achieve the standard of valid consent outlined in Article 6 (freely given, obvious, specific, withdrawable); **second**, get the consumer to confirm – oral or written – their agreement to the terms of the data processing.
Vital interests	This is used where processing is needed to protect life (including the consumer and other people). Where special category data is processed, this only applies if the individual is viewed as being incapable of giving consent at that point in time (which firms may conclude may also involve disclosures of suicide).

Sources: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation- https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/gdpr/lawful-basis-for-processing/

Substantial public interest: considering consumers

This lawful processing base requires firms to have clear and demonstrable reasons (rather than a general position or desire) why they cannot obtain explicit consent to process disclosed consumer health data.

Consequently, firms should be able to explain to regulators, staff and consumers alike:

1. **in which situations and in *what* ways a consumer's 'economic wellbeing' would be placed at risk if a firm were to attempt to obtain that consumer's explicit consent**.[6] This is about firms being crystal-clear about the situations where it is absolutely relevant, necessary and applicable to record the consumer's health data without explicit consent. Taking this step helps prevent 'economic wellbeing' being used as a 'catch-all' approach to processing all health disclosures, when in fact it might only apply to certain scenarios.
2. **how the *right* to object – where firms use the economic wellbeing base (Article 9) with the legitimate interests base (Article 6) – will be enacted at the point of disclosure.** Under this, consumers have a **right to object** to their data being processed and it is important they are made aware of this by firms at the earliest possible point (including – as we see below – explanation of how firms can override an objection in certain situations.
3. **in *which situations* and in *what ways* firms would override objections to processing**. Here firms need to make clear what constitutes a compelling ground for them to still record, retain and use a consumers' disclosure even where they objected to this data processing.

And under the GDPR 'accountability' principle, firms will need to collect monitoring data on received/upheld/overridden consumer objections to ensure a fair and transparent process.[5] Firms should also consider consumer harm that could be caused by overriding an objection (e.g. distress and fear about how the data will be used, leading to poorer mental health).

Under the GDPR, an explanation of the above needs to happen during a firm's first communication with a consumer, and be presented clearly and separately from other information.

Section two

LISTEN TO CONSUMERS' VIEWS

What do consumers think about data recording?

Discussions about data protection often fall into issues of compliance, technicality and possibility. This is understandable – firms want to comply with wider regulation, and many issues are complex.

However, in doing this, such discussions can overlook the views that consumers may have about the data processing approaches being considered by firms.

This is an oversight. While consumers are unlikely to speak the technical language that can accompany data protection debates, they will usually be best placed to understand how they want their data treated, and the harm this can cause where this does not happen.

Key scenarios

For this reason, in this section, we present data from qualitative interviews with people who have previously disclosed their mental health problems to essential service firms.

These individuals were asked for views on four different responses to a disclosure being made. They were asked to consider where a firm recorded a mental health disclosure:

1. without explaining how it would be used or asking for explicit consent to record this
2. with an explanation of how it would be used, but without asking for explicit consent
3. with an explanation of how it would be used, and asking for explicit consent to record this
4. with an explanation of use, and offering the right to object to data processing (noting this may be overridden).

What this can tell firms

Critically, our intention here is not to comment on how often consumers may have experienced or encountered one of these four approaches.

Rather, we want to encourage firms to do two things:

1. consider how the consumer views that are presented here – which touch on features of the lawful bases outlined earlier – might reflect views in their own consumer base
2. assess whether such views are being taken into account when decisions are made about the types of explanations or choices given to consumers making mental health disclosures.

Importantly, this is about ensuring that data processing approaches aren't just about what is technically possible or legally compliant in order to meet a firm's operational objectives, but also to take into account what consumers need in relation to understanding, support and control.

When no explanation or choice is given

The first scenario participants were asked about involved them making a mental health disclosure which was recorded by a firm without explanation or consumer permission to do so.

Experience

Notably, some participants reported that they had encountered such scenarios in real-life where firms referred to data on their systems that consumers had not agreed could be recorded:

> "I contacted [firm name] and they… didn't ask for my consent, but… they'd said, 'Yeah, we can see that you're going through this'. Being reminded of the situation that you are in… then knowing this person, this stranger has access to that information when you've not given consent to the company to keep it… there are untold consequences…"

For this participant, this was reported as potentially causing them stress, paranoia and an aversion to making further disclosures to firms in the future. Meanwhile, other participants explained they had not only encountered this, but had assumed such approaches were 'normal firm practice':

> "It'd be nice for them to… [explain and ask for permission], but I wouldn't have expected either of them. I thought it would be an automatic response [to me]… telling them."

Such experiences and views – as we will see in other scenarios – represented a persistent minority of consumers who were unclear about the data processing principles firms were required to meet, and unaware of their own rights under the GDPR.

Preferences

Among other participants, such an absence of explanation and choice was seen as unacceptable:

> "They've got to tell you, haven't they? They can't not tell you."

> "I would expect them to ask my consent to say, 'I'm gonna use this information'… rather than… just recording it anyway without consent."

For these participants, there was no case or 'best interests' reason why they felt their disclosed data could be recorded without an explanation, or without their permission.

> "if somebody said to me, 'I'm doing it in your best interests… how are you qualified to do that, you know? I might not want you to decide in my best interests… When, in actual fact… they're only doing, really, what's best for them".

And for one participant, acting without this permission was even akin to ‘theft’ and ‘deception’:

> “It feels like stealing information… It would make me angry because that’s still being deceitful. It’s not being upfront and honest.”

What should firms do?

It is hoped that few firms follow such a ‘don’t explain, don’t ask’ approach to processing mental health disclosures. However, the above consumer views indicate that firms should:

- review whether this might inadvertently be the case
- ensure that consumers are aware and informed their data is being processed
- consider how best to allow consumers a choice over whether their data is processed or not.

When an explanation is given, but not a choice

The second scenario involved disclosing consumers being given an explanation of how their data would be recorded, but with no choice about whether this recording could take place or not.

Choice is important to consumers

Most participants were not comfortable with the absence of a choice over their disclosed data:

> "I wouldn't be happy at all and I'd take the matter further, definitely. Well, they should ask permission first, really, shouldn't they, 'cos it's, it's something very sensitive".

This discomfort was – for some participants – accompanied by puzzlement about why firms might explain how disclosed data would be used but would then not offer participants a choice to decide whether to proceed on this basis:

> "I feel like, if they're going to explain how they're going to use the information, then they might as well ask you for your consent. [I]t seems like an odd thing to do – to tell someone how you're going to use their information, but then not give them a choice… you know, in whether they use that information in that way or not.

In practice, it is again hoped that such a situation would not occur (except where a consumer's life, or someone else's, was at risk – and where a 'vital interests' lawful basis could be used to do this).

However, what is significant here is the insistence by most participants that only they should be able to decide whether their data is recorded – a theme that we return to below.

Unaware that choice was a possibility

Again, those familiar with data protection issues might assume that most consumers are broadly aware of what might be expected of firms. However, some interviewees were not aware that firms could even offer consumers a choice over how their data were processed:

> "I don't think I'd understand that there's a… requirement on them to ask for my permission. That's interesting. You've made me think there, because I think you're the first person to say that, which is really interesting…"

Accessible explanations

Finally, some participants noted that when disclosing their mental health situation to firms, they had often been unwell. However, despite this, the explanations and information they had received, as well as the processes they were expected to subsequently follow, had been inaccessible to them.

For some this related to difficulties in remembering information verbally provided by staff (lending weight to calls for written summaries to be provided in certain situations), while others talked about written information being difficult to understand, or in an inaccessible format.

What should firms do?

Building on our previous recommendations, firms should:

- consider the role that consumer choice plays in their processing of disclosed data
- review information, explanations, and processes involved in disclosure to ensure these are clear, fair and accessible.

When an explanation and a choice are both given

The third scenario involved participants receiving an explanation of how their disclosed information would be recorded and being given the choice over whether this processing could proceed.

Expected as standard

Most participants expected firms would give them this control over their health disclosures:

> “It’s actually sort of what I would expect these days, you know, because of [GDPR] and all that kind of stuff”

And for many of these participants, a strong link between ‘my data, my decision’ underpinned this:

> “I think it’s important if they’re going to record something because it’s my data, my information and it’s my choice if I want to share it with that company”

Choice is often associated with consent

When discussing data and choice, some participants directly referred to giving ‘explicit consent’:

> “I mean, they certainly should be asking for your explicit consent… because it’s very sensitive information and you might be happy telling the person that you’re speaking to, about… whatever’s going on, but you might not be happy to know that’s on your file and, really, anybody could go in and look at it.”

This strong consumer link between choice and consent is key. First, consumers may expect such explicit consent to be sought by firms following a disclosure. Second, for those firms that do not wish to use explicit consent, it may mean offering a different form of choice during a disclosure – such as the ‘right to object’ – which may be less familiar, understood, or acceptable to consumers.

Explanation and refusal

Finally, some participants noted that explicit consent to processing could not be obtained unless they understood what they were consenting to. Here, consumers referred to the importance of a clear explanation in making this possible, and where this explanation both offered reassurance and took into account the nature of mental health problems that had just been disclosed:

> “I appreciate knowing what’s gonna happen to my personal information…especially when it’s as sensitive as, you know, your ill health… The only thing… [is] the sooner I can get somebody off the phone, the better… So… if they said, you know, ‘Right, OK, we’ll use this for certain purposes and we’ll send you an email with those details,’ that would be fantastic.”

Meanwhile, in relation to refusals of consent, some consumers doubted if firms would respect this:

> "They'll just [record] it whether I consent or not".

What should firms do?

Building again on our previous recommendations, firms should:

- consider the role that consumer choice plays in their processing of disclosed data
- offer accessible and reassuring explanations to consenting and non-consenting consumers (including what will happen in terms of support if a consumer does not give consent).

When an explanation and an opportunity to object are both given

The fourth scenario involved participants receiving an explanation. However, although given an accompanying choice over whether their data was recorded, this was not via explicit consent.

Instead, consumers were given a right to object to their data being processed (but with the caveat this right could be overridden by firms if a firm felt it had a compelling case to record the data).

First take: undermined

While interviewees initially welcomed the opportunity to object to processing, this position changed once they understood – that in certain circumstances – their objection could be overruled:

> "Oh, no, no, that shouldn't be done, definitely not… cos I've specifically said that I don't want it recorded and everything like that."

> "No, I don't like that. [If], if I have objected, then I have objected to my data being used in that way. I don't, I wouldn't like to think that they can make a decision about my mental health issues better than I can."

Even though participants were told that firms could only do this in certain circumstances (such as recording data to protect consumers from economic harm), this did not temper responses. Here, there was a sense that only interviewees could know what was 'best for them', rather than firms:

> "I'd feel undermined. I'd say I'm intelligent enough to know what's in the best interests for me. Even though I'm struggling with mental illness, I've still got capacity. I'm still intelligent enough to understand and… it's down to me whether I want you to record that information or not."

Reflection: physical harm and overspending

Participants were asked, however, if they could identify any circumstances where a firm should override a consumer's objection to their disclosure being recorded.

Some interviewees identified suicide or serious physical injury as a situation where objections to data recording could be overridden (a scenario catered for in the 'vital interests' lawful base):

> "If there was harm coming to me. If I was gonna harm myself, really."

Meanwhile, other participants cited episodes of overspending as a scenario where financial firms recording this detail might help, and where overriding objections could be valid. However, this came with one caveat: such an overriding of objections to record data should only take place if support could then be consistently provided by a firm to prevent the identified harm. In essence, overriding an objection, recording data, but not providing support was seen as unacceptable.

What should firms do?

Building on our previous recommendations, firms should:

- recognise that consumers feel they are best placed to make decisions about their own data
- understand that many consumers will not immediately understand what ‘the right to object’ to data processing means and involves (and careful explanation will be needed)
- acknowledge that if reasons do exist for overriding a consumer processing objection, these situations or circumstances need to be carefully defined – blanket or general statements stating that ‘economic harm’ will be prevented may not be enough for consumers.

About how much data should be recorded

In addition to the four processing scenarios outlined in this report, interviewees were also asked about what data they felt firms should record from a disclosure about their mental health situation.

Reflecting the GDPR's emphasis on only recording data which is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed", interviewees wanted firms to record the minimum of the most relevant data to inform meaningful action.

Adequate

Adequate data recording involves firms having the right amount and quality of data to support consumers disclosing a mental health problem. Capturing immediate support needs, or needs that may develop over time, was key to consumers. Where this information hadn't been recorded in the past, and needs weren't met, consumers reported experiencing poor mental health because of this:

> "There were certainly things that they... could've done to help me... [which] would've prevented [my relapse]."

Relevant

Relevancy is about only collecting information that directly informs the action and support a firm gives to a consumer (rather than being generally recorded 'out of interest'). As consumers noted, recording relevant data about their support needs helped improve their later interactions with firms:

> "They've put it on file, so… whenever anybody… contacts me, it's there so the person can see [and] understand what they're dealing with before [they] phone."

Limited

Finally, limiting the amount of data recorded about a consumer's disclosed mental health situation was seen as an important safeguard. Participants valued firms only recording what was needed for current action and support, with this seen as preventing organisations from collecting more and more data about a person's situation over time. After all, as one interviewee wryly noted:

> "Are they going to have a contact number for your psychiatrist?"

What should firms do?

Firms should record the minimum of relevant data to provide a consumer with support such as:

- what difficulties a consumer with mental health problems might experience including:
  - things that make it harder to fairly choose, purchase, access, use, talk with, complain about, pay for, or benefit from a product or service
  - things not related to a product or service, but where a firm can either (a) still take internal action to help, or (b) signpost or refer to external specialist agencies.
- any consumer views on what support could help this situation such as:
  - adjustments to process or changes to contact methods
  - or any contextual information that is relevant and could help provide this support
  - or assist a firm to take action to prevent, minimise, or avoid harm to the consumer.

Section three

RECOMMENDATIONS

What actions should firms take?

A number of lawful bases exist to process disclosed health data under the GDPR and DPA (2018).

This guide has focused on explicit consent (established and used across many sectors) and the newer lawful base of substantial public interest (which has attracted interest among some firms).

In doing this, we have provided an overview of the features of these two approaches, have set out their strengths and limitations, and have also – for the first time – offered insights into consumers' views about the choices and control they want to be given over their disclosed data.

Practical concerns

Our research recognises that firms may encounter some consumers who refuse explicit consent, and the risk of not recording such disclosures to prevent future harm is a practical concern.

However, we have also noted that approaches not based on explicit consent can have other risks. These include removing consumer choice, overriding consumer objections without compelling grounds, and using the base for processing all health disclosures, rather than in defined situations.

Consequently, our recommendations are:

Every firm should:

- know its reason or purpose for recording data from mental health disclosures
- ensure that staff know and can give clear and accessible explanations to consumers about how their disclosed data will be recorded, stored, used, shared and processed
- understand the foundational GDPR principles and individual rights and communicate these to consumers – where appropriate in a disclosure – to ensure fairness and transparency
- fully understand the definitions, strengths and limitations of the lawful processing bases that can be used to process data from a consumer mental health disclosure
- ensure that – alongside operational objectives and legal considerations – the consumer voice and experience are taken into account when deciding upon a lawful processing base.

Firms using explicit consent should:

- ensure consumers are told during disclosure that their explicit consent for data processing can be withdrawn at any time.

Firms considering the substantial public interest base should:

- have clear and substantiated reasons – rather than a general 'catch-all' position – why they cannot obtain explicit consent to process consumers' disclosed health data including:
    - in which situations and in what ways a consumer's 'economic wellbeing' would be placed at risk if a firm were to attempt to obtain that consumer's explicit consent
    - how the right to object – where firms use the economic wellbeing base (Article 9) with the legitimate interests base (Article 6) – will be enacted during disclosure
    - in which situations and in what ways firms would override objections to processing (including reflection on whether harm might be caused by overriding an objection).
- be aware that disclosure management tools – like TEXAS (see Guide One) – need adaptation to move from an 'explicit consent' to a 'substantial public interest' lawful processing basis (these adaptations are explained in detail in 'Vulnerability, GDPR, and Disclosure' by the Money Advice Trust and Money Advice Liaison Group).

Methodology

Interviews

Thirty-four telephone and in-person semi-structured interviews were conducted with frontline staff (n=13) and leadership in debt collection firms (n=7), and people with experience of mental health problems, debt, and debt collection (n=14).

Lived experience participants were recruited through an advertisement sent to selected members of Money and Mental Health Policy Institute's Research Community. Frontline staff and leadership participants from debt collection firms were recruited from one large sized firm, one medium sized firm, and two small sized firms. This firms were randomly selected using a sampling frame constructed for a separate quantitative survey study that is described further in Evans et al (2018).[7]

Interviews were conducted between December 2019–February 2020, qualitative data analysis ran from November 2020–February 2021, and write-up took place in 2021.

Survey

Money and Mental Health commissioned Opinium in 2021 to ask 5,001 adults (aged 18-65) who had experienced mental health problems about their lives, the largest ever representative online survey about money and mental health. The results of this survey are published in the Money and Mental Health report, 'The State We're In' (2021).

Acknowledgements

With a huge thanks to all the interview and survey participants who shared their time, insight, and experiences with the research team. And with additional appreciation to Jamie Evans and Sharon Collard (Personal Finance Research Centre, University of Bristol), Claire Henderson (Institute of Psychiatry, Psychology and Neuroscience, King's College London), and Rob Bell and Colin Trend for their support in the work, research, and thinking underpinning this series of guides.

References

1 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

2 Fitch C, Bell R and Trend C. Vulnerability, GDPR, and disclosure. Money Advice Trust and Money Advice Liaison Group. 2020. See also Fitch C, Evans J and Trend C. Vulnerability: a guide for debt collection. 21 questions, 21 steps. University of Bristol, Personal Finance Research Centre. 2017

3 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

4 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

5 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

6 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

7 Evans J, Fitch C, Collard S, Henderson C. Mental health and debt collection: a story of progress? Exploring changes in debt collectors' attitudes and practices when working with customers with mental health problems, 2010-2016. J Ment Health. 2018 Dec;27(6):496-503.

Permission to share

For commercial use, please email contact@ moneyandmentalhealth.org

MONEY AND MENTAL HEALTH
POLICY INSTITUTE

MONEY
ADVICE TRUST

Registered charity number 1166493

www.moneyandmentalhealth.org