MALG

Money Advice Liaison Group

Working together to improve the lives of people in debt

BRIEFING NOTE 4

APRIL 2013

Appropriately processing data from individuals with mental health problems under the Data Protection Act (1998)

Executive Summary

- This Briefing Note makes practical recommendations on the steps that creditors, their agents and debt advisers can take to fairly and legally process data from an individual who discloses a mental health condition.

- It has been developed following requests for clarification from banks, debt collection companies and debt advisers about the processing of sensitive personal data from individuals who disclose a mental health problem (as described in the MALG *"Good Practice Awareness Guidelines for Consumers with Mental Health Problems and Debt)".*

- The Briefing Note has been developed with the **Information Commissioner's Office** (to help ensure compliance with the Data Protection Act 1998) and shared with the **Office of Fair Trading and The Lending Standards Board**.

- The Briefing Note arises from (and is a further extension of) the MALG guidance document detailed above and the Royal College of Psychiatrists' and Money Advice Trust's '*Debt collection and mental health: ten steps to improve recovery'*.

KEY MESSAGES

1. **Organisations have a legal duty under the Data Protection Act (DPA) to fully explain to individuals how information about their mental health problems will be processed**. **The ICO says:**

   ***"If creditors want consumers to communicate with them and be open and honest about the difficulties they face in repaying their debts then they themselves will need to be** upfront about how they will process the data when it is volunteered to them...Getting a clear message out to creditors about the importance of being clear and transparent about how their customers' personal data will be processed is an extremely important message."*

   Practical implications: for organisations to be able to explain how data are processed to individuals, they will benefit from developing and establishing **a written mental health policy.** This will help staff to clearly explain (a) how data about a person's mental health problem will practically be used; (b) how data will be stored and shared; (c) how long data will be retained for, and how (if it is necessary to keep data for a period of time) it will be updated to ensure it is relevant, accurate and timely; and (d) how data will be disposed of.

   Policy note: organisations(a) should not automatically assume that it is 'reasonably obvious' to an individual who shares information about a mental health problem how this data will be processed, and (b) should not automatically conclude that an explanation is therefore not required.

2. **Data about a person's mental health are defined as *sensitive personal data* – legally, it must be treated with much 'greater care'. Consequently, the fairest way for organisations to comply with the DPA is to obtain the *explicit consent* of the individual**. **The ICO says:**

   ***"If individuals know at the outset what their information will be used for, they will be able to make an informed decision about whether to enter into a relationship. Assessing whether information is being processed fairly depends partly** on **how it is obt**ained."*

   Practical implications: informing individuals how their data will be processed is a fundamental requirement of the DPA. This full explanation is also the first part of *'explicit consent'*. The second part is the individual indicating that they understand the conditions for processing, and giving their consent for this to continue. Used alone, a written or oral Privacy Notice is insufficient – instead, a discussion with the individual (giving them the opportunity to raise questions or concerns) is recommended.

Policy note: technically there is an exemption under the DPA which provides an alternative to seeking *explicit consent* (Schedule 3) where processing "*is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights*." ***However***, the ICO has stated:

> *"[This] exemption could be easily misinterpreted to mean something other than the narrow application that it should have in practice. It needs more than just the possibility of legal action; it requires the decision to take legal action to have already been made."*

3. **The minimum of sensitive personal data about an individual's mental health should be held, and if held for an extended period of time, the data should be routinely reviewed to ensure it remains accurate.**

- This Briefing Note recommends the practical steps that creditors, their agents and debt advisers can take to fairly and legally process data from an individual who discloses a mental health condition.

- Divided into four sections, it has been developed through close dialogue and discussion with the **Information Commissioner's Office** to help ensure compliance with the Data Protection Act 1998[1]. The four sections make the following points:

  1. ***Collecting relevant mental health data is good practice***. All organisations should be collecting mental health data where this is relevant to the decisions and actions that need to be taken, and where undertaken in compliance with the Data Protection Act (DPA) and best practice industry guidelines.

  2. ***There is a legal duty to explain.*** Organisations have an over-arching responsibility under the Data Protection Act to fully explain to individuals how their mental health data will be used, processed and shared. Acting in this manner treats the individual fairly and ethically.

  3. ***Explicit consent is the fairest option.*** Organisations have additional responsibilities under the DPA to process ***sensitive*** personal data such as mental health information with greater care, and obtaining ***explicit consent*** provides the fairest option for meeting these responsibilities.

  4. ***It is necessary for organisations to hold the minimum of sensitive personal data, ensure it remains accurate, and keep this only for as long as is necessary.*** Organisations have the responsibility under the DPA to record only relevant and accurate data about a person's mental health problem, and is not kept on record for longer than is necessary.

- Sections 2, 3 and 4 outline the relevant parts of the DPA, provide verbatim guidance from the Information Commissioner's Office, consider the practical implications of this guidance, and address technical questions related to potential processing exemptions.

1. Collecting relevant mental health data is good practice

- We believe that it is *critical that organisations do collect relevant data* about an individual when information about a mental health problem is disclosed or made available to the organisation. Collecting relevant information is good practice as it:
  - allows creditors, their agents and debt advisers to make informed decisions
  - enables subsequent dealings to proceed as efficiently as possible because all the information is readily available
  - is especially beneficial with an issue such as mental health, where it can be difficult or intimidating for individuals to disclose a mental health problem, or for staff to identify, ask about, or discuss such mental health problems
  - allows creditors, their agents and advisers to be more responsive to an individual's circumstances
  - saves individuals from having to repeatedly disclose this information (which can be traumatic, difficult, and runs the risk of a disclosure not being recorded)
  - allows an individual's mental health to be taken into account in a way which assists both the commercial recovery of the debt *and* which also contributes to the personal and health recovery of the individual concerned

- ***However, the processing of such information must be undertaken in compliance with the Data Protection Act and in a manner which builds trust and rapport with often vulnerable individuals.***

[1]We would like to acknowledge the assistance of the Information Commissioner's Office, the Office of Fair Trading, the Lending Standards Board, the MALG Steering Committee, Diane Williams (The Capital Partnership), Colin Trend (debt adviser and member of the MALG Mental Health Working Party), Diane Forster (Head of RSG Compliance, Shoosmiths, Solicitors) and Jeremy Chaplin (Contested Litigation Manager, GPB Solicitors & Chair, Legal &Technical Committee, Civil Court Users Association).

2.1 What does the Data Protection Act say?

- Under the Data Protection Act, there is a ***fundamental and over-arching*** requirement for organisations to always collect, use, retain, or dispose of personal data both fairly and legally.
- One aspect of this requires the organisation receiving the data to tell individuals providing such information how it will be processed and used (there are several ways to do this - see below).
- Guidance accompanying the Data Protection Act indicates that the duty to explain is strongest when the information is likely to be used in an unexpected, objectionable or controversial way, or when the information is confidential or particularly sensitive.

Source: http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_1.aspx

2.2 What does the Information Commissioner's Office say?

- Following discussions with the Information Commissioner's Office from May 2012 onwards, the following statements were made by the ICO:

> *"Processing personal data must be fair, and fairness generally requires you to be transparent, clear and open with individuals about how their information will be used.*
>
> *"If creditors want consumers to communicate with them and be open and honest about the difficulties they face in repaying their debts then they themselves will need to be upfront about how they will process the data when it is volunteered to them..."*

2.3 Practical implications

- Establishing a **written mental health policy** will help ensure that all staff in an organisation clearly and consistently explain to the individual how data about an individual's mental health will be used and processed.
- To develop such a policy, it may be helpful for an organisation to:
    a. 'take stock' of how they currently work with individuals with mental health problems – this could include reviewing key steps in the individual's journey to consider (i) what action staff take in relation to mental health and (ii) what information is collected when this happens (see **BOX 1** for an example 'check list')
    b. ensure that consideration is paid to (a) how data about a person's mental health problem will be used, stored, and shared; (b) how long data will be retained for, and how (if it is necessary to keep data for a period of time) it will be updated to ensure it is relevant, accurate and timely; and (c) the criteria determining when and how data will ultimately be disposed of
    c. align this practice with the (i) DPA and other relevant legislation, (ii) industry codes of practice and (iii) wider guidance documents (see below)
    d. identify both what the organisation already does well, and where existing organisational practice could or should be strengthened
    e. write an organisational policy based on this exercise, which will clearly describe to staff (i) what action to take when encountering an individual with mental health problems, (ii) what information will need to be collected about that person, and (iii) how that information will be used, stored, shared, and ultimately disposed of
    f. communicate this policy to all staff on regular occasions (including training)
    g. require staff to explain relevant aspects of this policy in clear and straight-forward language to individuals with mental health problems, and to answer any relevant questions that individuals may have about this
- Taking these steps will help organisations comply with the Data Protection Act, and will help staff treat this group of individuals fairly and sensitively.

'Taking stock': what to consider?

When 'taking stock' of how they currently work with individuals with mental health problems, organisations may find it useful to consider how well staff:

- manage initial disclosures of a mental health problem
- explain to individuals how any information about their mental health will be used
- obtain *explicit consent* from individuals to process their data
- ask questions about the mental health problem (and whether this will help the organisation make informed decisions)
- record data about an individual's mental health problem
- work with (and refer to) any internal staff/teams with specialist expertise in mental health
- collect and use medical evidence to aid decision-making
- work with third parties (such as carers or other agencies)
- deal with difficult situations (e.g. suicide threats)
- work with (and refer to) any external organisations (e.g. NHS 111 or the Samaritans)

Organisations will find it useful to consult guidance such as:

- the Royal College of Psychiatrists and Money Advice Trust's *'Debt collection and mental health: ten steps to improve recovery'* (www.rcpsych.ac.uk/recovery).
- the Money Advice Liaison Group's guidance document *'Good Practice Awareness Guidelines for Consumers with Mental Health Problems and Debt'*(www.malg.org.uk/debtmentalhealth)

2.4 Policy note

- Guidance on the Data Protection Act does state that it is not necessary to provide such an explanation in situations where it would be obvious to the individual how that data will be used, or in ways that individuals might reasonably expect.
- *However, there are three reasons why this would not apply to individuals sharing information about a mental health problem:*
  a) robust evidence exists that it is neither obvious to individuals with mental health problems, or frontline debt collection staff, how such data would be processed (see **BOX 2**)
  b) the collection of health data by creditor, debt collection agencies, or advisers is a relatively new development, and it is arguably neither obvious to individuals (nor reasonably expected) why such information would be collected
  c) individuals with mental health problems may experience difficulties in understanding how such information will be processed due to their condition, or may not have the mental capacity at the time of contact with the creditor to understand.

3. Explicit consent – the fairest option

3.1 What the Data Protection Act says...

- The Data Protection Act requires data which is of a very private or sensitive nature to be treated with greater care than other personal data.
- Physical or mental health is classed in this way as 'sensitive personal data', sitting alongside data, for example, on race or ethnicity, religious beliefs, sexuality, offending and criminal history.
- Such sensitive personal data can only be processed if the organisation receiving the data (a) meets at least one of nine conditions; and (b) ALSO processes that data in a fair and legal manner.
- The first of the nine conditions in the list is that the individual who has provided the sensitive personal data has given their ***explicit consent*** for it to be processed[2].
- *Meeting this condition is the fairest way of ensuring that creditor and adviser organisations meet the requirements of the Data Protection Act.*

[2]For further information, please see www.ico.gov.uk/for_organisations/data_protection/the_guide/conditions_for_processing.aspx

BOX 2

The Royal College of Psychiatrists and Mind have twice collaborated on research with individuals with debt and mental health problems. Drawing on a study conducted with 924 individuals, and asking them about their experience of working with creditors and debt collection organisations:

- 40% of those individuals who did not tell their creditor about their mental health problem, said this was because they were concerned about what [the creditor] would do with the information about their mental health problem
- only 4% of those individuals who did tell their creditor about their mental health problem said they were clearly told what would happen to any information they provided about their mental health problems

This represents a situation where it is not at all clear to individuals with mental health problems how their data will be processed. Furthermore, individuals may be deciding *not* to engage with organisations about their mental health problems, due to a perceived lack of transparency and trust about data processing.

Source: Mind 2008

3.2 What does the Information Commissioner's Office say?

- Following discussions with the Information Commissioner's Office from May 2012 onwards, the following statement was made by the ICO:

> *"If individuals know at the outset what their information will be used for, they will be able to make an informed decision about whether to enter into a relationship. Assessing whether information is being processed fairly depends partly on how it is obtained."*

3.3 What are the practical implications?

- *Explicit consent* is not defined in the Data Protection Act but is essentially comprised of two parts:
  - the first part is fully explaining to individuals why their information is being collected, how it will be used to help decision-making, and who (if anyone) the data will be shared with/disclosed to
  - the second part is asking individuals whether they understand this explanation, and whether they consent or agree to continue with the processing of their data
- A recommended 'staff drill' for obtaining *explicit consent* is outlined in **BOX 3**. Wherever possible, consent should be in writing, but if it this is not achievable, an accurate note should be kept on the individual's file, once *explicit consent* is obtained, (which can be shared across relevant parts of an organisation).
- ***Used alone**, **a written or oral Privacy Notice is an insufficient means*** of informing individuals how their data will be processed – individuals need to be given the opportunity to raise questions or concerns, and a fuller discussion is required to ensure that the individual understands what they are consenting to. The advantage of offering this good practice is that the individual may gain confidence in being open, engaging with, and trusting the organisation concerned (thus creating good rapport), and it also shows fairness, understanding and transparency (which are required by the DPA).

3.4 Policy note: legal proceedings (creditors or debt collection companies)

- There is an exemption under the DPA which provides an alternative to seeking *explicit consent* (Schedule 3). This is where processing "*is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights*."
- However, while this represents a legal basis for processing data without following the best practice of seeking an individual's *explicit consent*, there are four important considerations which should be noted.

Firstly, the Information Commissioner's Office has warned that:

> *"[This] exemption could be easily misinterpreted to mean something other than the narrow application that it should have in practice.* ***It needs more than just the possibility of legal action****; it requires the decision to take legal action to have already been made."*

explicit consent.

This is because the process of *explicit consent* involves the organisation discussing in detail how the individual's mental health situation affects their ability to repay, which improves the chances of successful debt recovery and allows the individual's situation to be taken into full account.

Furthermore, the process of *explicit consent* also involves the organisation explaining to the individual how their data will be used – as explained previously; the lack of such an explanation can stop many individuals with mental health problems meaningfully engaging and building trust and a relationship with organisations.

Thirdly, taken together, the above two points mean that organisations <u>should not</u> view the exemption of 'legal action' as a convenient method of 'opting-out' or 'avoiding' having to obtain explicit consent.

Even where legal action is being pursued, there are real intelligence and collection benefits in obtaining *explicit consent*, rather than avoiding this. Furthermore, even in those situations where organisations do not wish to, or cannot obtain *explicit consent*, there still has to be credible evidence that the organisation is actually pursuing legal action.

Fourthly, even where (a) strong practical grounds for the exemption exist and (b) the data controller decides that on balance they should proceed, organisations still have to comply with other parts of the DPA. As explained in Section 2, this includes the over-arching legal duty to process data fairly which means individuals still have to be provided with an explanation of how their data will be processed.

BOX 3

The report *'Debt collection and mental health: ten steps to improve recovery* 'provides a drill that organisations and staff could follow when an individual tells them about a mental health problem. This is called the **TEXAS** drill:

Thank them (what they have told you could be useful for everyone involved)

"Thanks for telling me, as it will help us deal with your account better"

Explain how their information will be used (it is a legal requirement)

"Let me just explain how we'll use that information, so you know"

NB This includes why the information is being collected, how it will be used to help decision-making, and who the data will be shared with/disclosed to.

Explicit consent (it is a legal requirement)

Now ask the individual for their permission to use their information in this way

Ask three key questions (these will help you understand the situation better)

1. Does your mental health problem make it difficult to repay your debt? If so how?
2. Does your mental health problem affect your ability to deal or communicate with us? If so how?
3. Does anyone need to help you manage your finances such as a carer or relative? If so how?

Signpost to internal or external help (where this is appropriate)

At this point, staff and organisations might:

- need to internally refer the individual to a specialist team/staff member in their organisation
- creditors or their agents may want to consider external signposting to an organisation such as:

a debt advice agency for help with multiple debts

NHS 111 for more help with a mental health problem

the Samaritans (0845 790 9090) for suicidal or despairing people

3.5 Policy note: situations where repeated attempts to obtain *explicit consent* have failed

- There may be rare occasions where:

- despite genuine, full and repeated attempts by a creditor/adviser to obtain an individual's *explicit consent* to process sensitive personal data about their mental health problem, this *explicit consent* cannot practically be achieved[3];
- despite genuine, full and repeated attempts by a creditor/adviser to work with (and support) an individual, the individual repeatedly gives then withdraws their *explicit consent* for the processing of their sensitive personal data[4].

- In such situations, if (a) the creditor/adviser has fully documented their efforts to obtain the individual's *explicit consent*, (b) reasonable support has been offered or provided to the individual to help them give this consent, and (c) all other aspects of compliance with the Data Protection Act and other relevant legislation are in order, then the creditor/adviser may decide to process this information without obtaining the individual's *explicit consent*.
- On this matter, the Information Commissioner's Office has stated that:

  "If the processing is not otherwise unfair or in breach of any legislation and if there is a strong case for processing without consent then the data controller may decide that on balance they should go ahead. It is still possible that a breach of the 1st Principle [of the Data Protection Act] might arise. The Information Commissioner's Office expects a data controller to have a clear rationale and strong justification for continuing to process the data. The best interests of the data subject should be the key consideration. The Information Commissioner's Office will take the data controller's rationale and justification into account if investigating a case in which the decision to process data without consent has been challenged by the data subject."

4. Data processing: data quantity, quality and time held

4.1 What the Data Protection Act says...

- The Data Protection Act states that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- The Act also states that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. The data should also be accurate and, where necessary, kept up-to-date.

4.2 What does the Information Commissioner's Office say?

- The Information Commissioner's Office has said:

  "We would also expect care to be taken that the data captured and shared are accurate, up-to-date and not excessive. It might not always be necessary to hold specific details about the individual's mental health problems in order to treat them fairly. Creditors need to be very cautious about holding and sharing unsubstantiated comments or opinions. Having clear policies and procedures in place may help staff to recognise what data to record and how they should do this."

  "Firms should [also] be careful not to go too far the other way and hold inadequate information about why they are dealing with a customer in a particular manner."

4.3 What are the practical implications?

- The minimum of sensitive personal data about an individual's mental health should be held – organisations (creditors, their agents or advisers) should aim to strike a practical balance between having 'enough' relevant information to inform decision-making, while avoiding recording an excessive amount of personal and sensitive information.
- If held for an extended period of time, data should be **routinely reviewed** to (a) check whether the data needs to be retained (i.e. is there a valid reason for continuing to hold the data in its current form); and

[3] An example would be where (a) an individual has written to a creditor and disclosed a mental health problem (b) the creditor has attempted to contact the individual to obtain their *explicit consent* to process this sensitive personal information (and to also find out more about its impact and relevance on repayment), but (c) despite genuine, full and repeated attempts, contact cannot be established with the individual. Where an account is going to be passed/sold to a debt collection agency or debt purchase company, this could result in relevant information about this potentially vulnerable individual not being shared with that agency, and not being taken into account during further collections activity. It should also be remembered that under The Lending Code a debt arising from an individual with mental health problems, should not be sold.

[4] Creditors and advisers should always consider what support an individual may need to give their *explicit consent*, particularly where the individual may have a mental or physical disability, or where they may be experiencing a limitation in their mental capacity to make a decision.

description of the individual's current situation.

- In regard to the latter point, we understand 'up-to-date' and accurate information as data which reflects the individual's current situation, or strictly relevant details of a past state. This is particularly important in relation to mental health because conditions can 'fluctuate' and vary in their effects over time.
- The Information Commissioner has confirmed again that sensitive personal data on the individual should be regularly reviewed and if the person has fully recovered, or, in the opinion of the data controller, there is no longer a requirement to keep the data, it should be deleted; if on the other hand the mental health condition remains, or it would be detrimental to the data subject to delete it[5], then the sensitive personal data can be held for as long as is justifiable and necessary.

5. Conclusion

- We believe that it is critical that in debt collection situations that organisations *do collect* information about an individual's mental health problem when this is disclosed or discussed.
- When doing this organisations should:

1. ***Explain.*** Organisations are obliged under the Data Protection Act (DPA) to ***fully explain*** how an individual's mental health data will be used and processed.
2. ***Obtain explicit consent.*** Organisations have a heightened responsibility under the DPA when processing sensitive personal data such as mental health information. Obtaining ***explicit consent*** provides the fairest option for meeting this responsibility.
3. ***Engage with the individual concerned***. The process of collecting information about an individual's mental health problem, involves an opportunity to engage and understand their situation. This can help both those organisations involved in collection activity, and also advisers in taking the individual's situation into account.
4. ***Hold the minimum of sensitive personal data and ensure it remains accurate.*** Only relevant information for decision-making should be collected, and steps need to be taken to make sure that these data are accurate.

Authors

Anthony Sharp
Chair MALG

Chris Fitch
Research fellow
Royal College of Psychiatrists

Neither MALG nor the Royal College of Psychiatrists can make a policy, as such, within the debt and mental health arena. They can only recommend certain actions as being' best practice' and that is what we hope we have achieved.

[5]The Information Commissioner's Office has noted that data about a customer's mental health problem could be retained if it could be demonstrated that doing this was genuinely in the interests of that customer. Equally, where a creditor had a strong reason to document why they made a specific decision about a customer at a point in time when that customer was experiencing a mental health problem, this could justify retaining this historical data. However, in all cases such data should neither be inaccurate nor excessively detailed, and creditors should continue to regularly review the need to hold such information for extended periods of time.