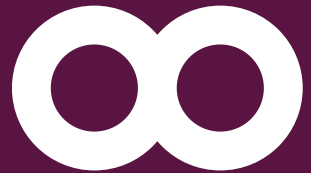




LOTTERY FUNDED



homeless link

CRITICAL MASS

FROM PRIVATE TO PUBLIC

**ETHICAL CONSIDERATIONS IN USING
OPERATIONAL DATA FOR NATIONAL RESEARCH PURPOSES
APRIL 2011**



WWW.HOMELESS.ORG.UK/CRITICAL-MASS

TABLE OF CONTENTS

1 INTRODUCTION.....	1
2 CURRENT PRACTICE IN SERVICES	2
2.1 CONSENT FORMS	2
2.2 POLICY AND PROCEDURES	3
3 LEGAL FRAMEWORK	4
3.1 THE DATA PROTECTION ACT.....	4
3.2 CORE PRINCIPLES OF THE ACT	6
3.3 OTHER REQUIREMENTS FOR ORGANISATIONS.....	9
4 CONSULTATIONS.....	10
4.1 CLIENT CONSULTATIONS.....	10
4.1.1 ACCESS AND IMPARTIALITY:.....	10
4.1.2 CONSENT AND CONFIDENTIALITY:.....	11
4.1.3 RESPONSES.....	11
4.2 PARTNER CONSULTATION.....	16
4.2.1 RESPONSES.....	16
5 PRACTICE IN OTHER SECTORS	18
5.1 NATIONAL TREATMENT AGENCY FOR SUBSTANCE MISUSE.....	18
5.2 DEPARTMENT FOR WORK AND PENSIONS.....	21
5.3 HUMAN TISSUE BIOBANK	23
5.4 RESEARCH BODIES	25
5.4.1 ETHICAL RESPONSIBILITIES TO SUBJECTS	26
5.4.2 GOVERNANCE AND ACCESS.....	27
6 PRACTICAL ASPECTS OF ANONYMISATION AND SHARING DATA	28
6.1 THE PROCESS OF ANONYMISATION.....	29
6.2 ISSUES TO ADDRESS BEFORE ANONYMISING DATA.....	31
6.3 LINKED ANONYMISED DATA	31
6.4 LIMITATIONS OF ANONYMISATION.....	32
7 CONCLUSIONS AND RECOMMENDATIONS	32

1 INTRODUCTION

This report forms a part of Homeless Link's Critical Mass project, a 3-year research project funded by the Big Lottery.

The central concern of Critical Mass is that there is no national data source that covers non-statutory homeless people at all stages of their journey, from living on the streets to moving into a home. The best proxy is Supporting People¹, but this only covers accommodation based services. Homeless Link's 2010 SNAP research showed that 95% of homelessness services use some form of client-recording system to monitor and report on clients' needs and outcomes achieved across all forms of provision.² Critical Mass will bring this data together for the first time to produce a comprehensive wider data set.

It is thought that client recording systems could yield powerful and valuable data but this has never been tested. Homeless Link has received funding from the Big Lottery to collate, combine and analyse client recording data from seven partners using In-Form³ and to report on the findings. The aim is to see if client recording data can be used to inform policy and practice.

As a part of Critical Mass we are looking at the ethical and legal considerations of using operational data for national research purposes. There has been no formal ethical oversight or guidelines for homelessness organisations who wish to explore how the personal data they gather through supporting clients could be used for research purposes, especially outside the organisation. Taking the data 'outside the organisation' could mean aggregation with data from other organisations, allowing social researchers to analyse data for any number of inquiries, and the archiving of data for future research purposes. As homelessness organisations have greater need and impetus to explore the development and use of social research data based on their operational data, a consistent approach to the ethical and legal concerns is required.

As homelessness organisations have greater need and impetus to explore the development and use of social research data based on their operational data, a consistent approach to the ethical and legal concerns is required.

This report explores the following questions:

- What is the current practice of data collection and use in frontline services?
- What is the legal and ethical framework?
- How do other sectors manage these processes?
- What are the ethical, legal and data quality considerations in anonymising personal data and using it for research outside the operational context?
- How will these issues impact on practice in services?
- How can we make it easier for services to address these issues?

This is a discussion document intended to assist homelessness services to identify and address a number of key legal and ethical issues as their operational data is moved from support purposes to research purposes. This document is not legal advice and should not be construed as such. Organisations are advised to seek legal advice as needed.

The client data being used in Critical Mass is used without the consent of the clients involved. We have undertaken two processes to manage the ethical issues arising from this use. Firstly, we have sought ethical oversight from St Andrews University, who will advise and guide on the ethical uses of this data for the duration of the project. Secondly, all data was anonymised before it was released to the researchers. St Andrews provided guidance on which fields needed to be eliminated and which to keep to ensure no individual was identified but meaningful data was retained. Issues of ethical oversight in research and practical aspects of anonymising data are discussed later in this report.

2 CURRENT PRACTICE IN SERVICES

2.1 CONSENT FORMS

We reviewed the consent forms used by the Critical Mass partner agencies. The forms were subjected to a 'closed comparison' whereby the similarities and variations between the documents were observed, but there was not a comparison to any 'ideal' consent document. The comparison is not a criticism of the consent documents, but a way to look at the different solutions various services have found to the same issue. From this selection of seven diverse organisations it can be extrapolated that there is considerable variability in consent practices across the sector.

Table A shows a summarised list of all the different clauses and information contained in all the consent forms. Where the issue was seen in a form the issue received a 1 'score' on the table. The final number in the 'evidenced in' column reflects the number of different consent forms who share this information or issue. As can be seen from the table, no single issue evidences a '7' illustrating that there was not one issue that was common to all agencies. A 'score' of 7 would not indicate a 'perfect' consent form, merely that all agencies had this issue in common on their forms.

The majority of consent forms were focused on ensuring the client had given permission for staff to record their personal details. The approaches varied from 'opt in' to 'opt out' choices (especially for information sharing external to the service). Consent forms reflected the needs of services in terms of the service they provided – the longer the residential service the more likely they were to have a more detailed consent form, possibly reflecting the both the intensity of support provided and the length of time they have to discuss these issues and complete paperwork with a client. The consent forms used in day centres covered the core permissions but were less detailed in terms of naming agencies with whom information will be shared, again, this likely reflects the support levels and different time-pressures experienced in a day centre setting.

Table A:

ISSUE	EVIDENCED IN
Why consent is requested	4.5
Obtaining information from specified organisations or professionals	4
Where / how info is kept	4
What sort of information is recorded	4
Sharing information with specified organisations / professionals / internally	4

How long information is kept for	4
Access to information about self and procedure for accessing	3.5
What the information is used for	3
Concerns about any aspect of this consent / keeping data and what to do	3
Refusal to consent (may) limit service	2
Opt out of some sharing / obtaining with specified professionals or agencies	1.5
Destruction of information	1
Refusal to consent does not limit service	1

1.0 allocated for definitely included in form

0.5 allocated for unclear / non-specified / incomplete inclusion in form

0.0 allocated for absent from form

The partners noted that the booking-in process, whereby clients are signed into the service, can be long and is generally quite paperwork heavy. It was noted that there is a lot of information for clients to take in at assessment and induction; this issue was explored further in consultation with clients.

Of key interest to this project was the lack of detail in the consent forms on how data may be used externally. The central focus was around what happens to the information within the service. In the context of the potential development of a national data set based on operational data from homelessness services there are issues to explore about what consent is required from clients to ensure the legal and ethical concerns are addressed and managed. The project partners stated that good practice guidance on consent processes would be helpful.⁴

2.2 POLICY AND PROCEDURES

Each of the partner agencies has formal policy and procedures for their staff outlining the actions and responsibilities of staff with regard to client confidentiality. The detail and length of the documents varies greatly, ranging from three pages to twenty seven pages.

As per Table A, Table B is a closed comparison between the policy and procedures documents supplied by six of the partner agencies. For the purposes of this report only the clauses related to client information have been included and other confidentiality issues (such as personal details of staff) have been excluded.

Table B

ISSUE	EVIDENCED IN
INTERNAL ORGANISATIONAL PRACTICE	
Explicit client consent required	4
Internal information sharing	5
Security of files	4
Appropriate physical privacy for discussing sensitive information, conducting keywork sessions, telephone calls, etc.	4
Internal monitoring – incidents, complaints, staff training, service user consent levels	1
Refusal or withdrawal of consent	2
Disposal of files	4
EXTERNAL / INTER-AGENCY	

Sharing personal information with other agencies with consent	6
EXEMPTIONS	
General	1
Medical reasons	3
Criminal or legal obligation	5
Defined Acts (eg Child Protection, Terrorism, Misuse of Drugs)	2
Risk of harm (including Protection of Vulnerable Adults)	3
Consent is not required under the DPA	1
LEGAL FRAMEWORK	
Data Protection Act – brief reference	3
Data Protection Act – detailed reference	2
Subject access to personal information	6
Human Rights Act referenced	2
ANONYMISED DATA	
Anonymised data for reports and/or research	2

As Table B shows, there were many differences between the partner agencies' confidentiality policy and procedures. Sharing personal information with other agencies and subject access to personal information were the only two areas where all six documents addressed the same issue. Even where there was commonality there was much variation in the level of detail provided. For example, although all partners included information on subject access in some instances this was a two-line reference and in others a detailed procedure for staff to follow was provided.

Whilst these policy and procedures documents fulfil legal requirements and provide overall parameters on confidentiality to staff, they are not particularly user friendly. All partners also provide training to staff which is likely to be more practical and flesh out the detail of the policy. In terms of front line staff a manual based on a 'frequently asked questions' format (potentially available online via local intranet) may assist in providing detail on procedures when the principles of the policy have been established and embedded.

It is interesting to note that only two partners explicitly mentioned the use of anonymised data. One agency referred to anonymised data as no longer being confidential and thus could be used for reports, statistics and research. In terms of developing a national dataset based on the information collected by individual agencies this type of clause will need to be included in consent and policy documents. Whilst there is no clear legal requirement to inform clients of the use of their data when anonymised there are ethical issues which arise about the need for informed consent.

The development of a standardised protocol or guidance for anonymising data would be useful for agencies both in terms of ensuring the quality of their data and being able to accurately inform clients about what information is used, even in anonymised form. These issues are explored in more detail in Section 6.0.

3 LEGAL FRAMEWORK

3.1 THE DATA PROTECTION ACT

Most homelessness services will be aware of their duties and obligations under the Data Protection Act (DPA/the Act). Because the Act forms the bedrock of the way organisations need to manage personal data it is worth taking time to explore the key

principles. This section therefore aims to give a brief overview of the Act, and discuss some of the main requirements of the Act in relation to the consent and ethics considerations of the development of a national data set on homelessness which is extrapolated from personal data.

In simplest terms, the Data Protection Act of 1998 is the framework of duties and rights which protect personal data. The Act applies to the activity of “processing personal data” rather than particular organisations or individuals, and the Act regulates such processing. This means that the need to comply with the Act is predicated on the activity being undertaken with personal data. Data must be processed in accordance with the Act. Central to the Act is the safeguarding of the data and the individual to whom the data belongs. Duties under the Act remain, and the rights of the subject must be upheld, until the data is returned, deleted or destroyed. The Act also covers how data is disposed in order to ensure the subject is not prejudiced as a result.⁵

The Data Protection Act is administered by the Information Commissioner's Office.

KEY TERMS

A brief selection of key terms from the Act are listed below. These terms describe certain processes and the relationship between parties in respect of the Act.

Personal Data: data which relates to an individual who can be identified, either directly from the data or in conjunction with other information the data controller may already have or may likely come into possession. This data can include opinions about the individual and indications of the intention of the data controller, or other people, with regard to the individual about whom the data relates.⁶

Sensitive personal data: The Act defines a second level of personal data – that which is “sensitive”. This is data about an individual that may consist of include information about their racial or ethnic origin; political opinions; religious beliefs; physical or mental health; sexual life; the commission or alleged commission of an offence by the subject; any proceedings for any offence alleged to have been committed by the subject, the disposal of such proceedings or the sentence of any court in such proceedings.⁷

Data Processing: is the obtaining, recording or holding of information (personal data or sensitive personal data) or carrying out any operation or set of operations on the information or data. This could include organising, adapting, altering, retrieving, disclosure by transmission or dissemination, alignment, combination, blocking, erasure or destruction of the data. Homelessness services, especially those using computer based systems for client data will recognise that they are indeed processing client data under this definition.⁸

Data subject: the individual about whom particular personal data relates. In this report the words 'individual' and 'client' are used largely interchangeably to refer to the data subject as defined by the Act.⁹

Data Controller: a person or persons who, alone or jointly, determine the purpose and manner of any data collecting. Data controllers will usually be organisations, but may be individuals (eg consultants).¹⁰ In this paper “homelessness services” and “organisations” are used in place of data controller for easier understanding of the relevance and implications of the Act.

3.2 CORE PRINCIPLES OF THE ACT

The Data Protection Act has eight principles, which are listed below, with notes on the principles which have particular relevance to homelessness services. All information is taken from The Guide to Data Protection produced by the Information Commissioner's Office.¹¹

Personal data shall be processed fairly and lawfully and in particular, shall not be processed unless -

a) at least one of the conditions of Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met

The key theme of this principle is transparency and legitimacy in how the data is collected and used. In the first instance organisations must have legitimate grounds for collecting and using the data. Organisations must be transparent in the way they intend to use data and provide clients with appropriate privacy notices in relation to this. It is the responsibility of the organisation to ensure that nothing unlawful is done with the data, and that it is not used in ways that would have an unjustified adverse effect on the client. This principle also asks that the organisation puts themselves in the position of the client and thus manage the data in ways the client would reasonably expect.¹² For homelessness services it is important to develop an understanding of what the 'reasonable expectation' of data management is for clients. Please see Section 3.1.3.1 Permission in this document for some feedback on this from clients during our focus groups.

This is the principle that sets out how information should be shared; fairness and transparency are the key themes of sharing personal data with other organisations. Clients must be told about the possibility their information will be shared and thus be able to make an informed choice about whether to share their information with the service in the first place.¹³

The "conditions for processing" in Schedules 2 and 3 are in addition to fair and lawful processing. The conditions become more exacting as the data being collected becomes more sensitive. The condition most relevant to homelessness services is that "the individual who the personal data is about has consented to the processing" – as such consent processes and documentation are a necessary part of the requirements of the Act.¹⁴

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.

The second principle is to ensure that organisations are open about their reasons for obtaining personal data and that what they do with the data is within the "reasonable expectations of the individuals concerned". An important part of this principle is that any further processing of the data must be compatible with the specified and lawful purposes already determined by the data controller. This is especially relevant to homelessness services and this project with the potential that data are further processed into a national data set.

As long as consent documents for clients address the potential further uses of the data and it is clearly compatible with the original specified purposes for obtaining that data then this principle is met. Currently specified purposes in homelessness services may be limited to supporting the client. The further uses or processing of client information is an area that current consent documents do not address as clearly as they could, and inclusion of a clause related to the use of data for statistics,

research and reports in anonymised form, and a plain language explanation of this, would be beneficial both to clients and to meeting the requirements of the Act.¹⁵

There is indeed a legal grey area here, as the DPA is only concerned with data that is personally identifying and anonymisation virtually cancels this possibility. However, the spirit of the principle is transparency in specifying the purpose of collection of the information and if that includes anonymisation for research or other purposes then there is an ethical duty to inform and seek consent.

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Principles 3, 4 and 5 the information standards principles and are the standards that must be met before data can be processed. Each of these principles is interconnected and a failure in any one is likely to lead to a failure in the others. In practice it means that organisations need to practice “data minimisation” - that the personal data held about a client is sufficient for the specified purpose and that no more information than is needed to meet that purpose is held. For homelessness services this is likely to be reflected in the training of staff about what information, and in what quantity, is appropriate to record.¹⁶

Personal data shall be accurate and, where necessary, kept up to date.

The second of the ‘information standards’ principles addresses accuracy and currency of data. Compliance with this section is through taking reasonable steps to ensure the accuracy of personal data obtained, consider carefully any challenges to the accuracy of information and whether it is necessary to update the data. The Act recognises different accuracy expectations of data obtained from the client or from third parties. An important part of this principle is acknowledging the source of data is relevant to its accuracy, for example stating that the source is a third party and then recording the information. This is especially important if the information is an opinion or the fact cannot be checked directly. This principle also acknowledges that errors and mistakes do occur and there may be a benefit to the client in correcting the information but also keeping record of the error, how it came about and how it was addressed. The Act does not say that every piece of information needs to be checked and updated but that this is related to what the information is used for – if the information is used for a purpose that relies upon it being current then there is an obligation to ensure it is kept up to date.¹⁷ For example, in homelessness services historical health information is likely to be static, but health services being accessed and health issues relevant to supporting the client currently will need to be checked and updated.

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

The Act does not define a minimum or maximum period for keeping personal data. In practice organisations will need to review the amount of time they keep personal data, in deciding whether and for how long to retain personal data organisations need to relate it to the purposes to which the data is put, secure deletion of personal data when it is no longer needed for the purpose/s and when information goes out of date it needs to be securely deleted, updated or archived. The implication for homelessness services is defining this in policy and procedures and making sure it is clear to clients in consent documents.¹⁸

Personal data shall be processed in accordance with the rights of the data subjects under this Act.

The rights given to data subjects under the Act are:

- the right to see the information held about them
- a right to object to any data processing that may cause distress or damage
- a right to claim compensation for damages caused by a breach of the Act
- a right to object to decisions undertaken by automated means
- a right (in certain circumstances) to have inaccurate personal data rectified or destroyed
- a right to prevent processing for direct marketing¹⁹

The rights most relevant to homelessness services in the context of this report are that clients have a right to see the information that is held about them and the right to object to any data processing that may cause distress or damage. As seen in Section 2.1 and 2.2 approximately half the partner organisations explicitly state this in their consent documentation and all agencies refer to this in their confidentiality policy and procedures.

The protection of the data subject from harm is a thread running through the entire DPA and is the key principle in any collection and use of an individual's personal information. For homelessness services this

The protection of the data subject from harm is a thread running through the entire DPA and is the key principle in any collection and use of an individual's personal information. For homelessness services this has a natural fit with their safeguarding responsibilities, and responsibilities around personal information should therefore be seen as an extension of such safeguarding.

has a natural fit with their safeguarding responsibilities. The responsibilities around personal information should therefore be seen as an extension of such safeguarding.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

This section of the Act is concerned with security of data. The key points are that organisations need to ensure security fits the nature of the personal data being held – very sensitive data requires very strong security. There should be clarity in the organisation about who is responsible for data security and make sure that the appropriate physical and technical security measures are in place. Further to this there must be strong policy and procedures and staff trained in the use and importance of these measures.²⁰

Computerised databases for managing client data such as In-form have significant security features built in, starting with complex password systems and time-outs. The focus groups we conducted with clients (see section 3.1) indicated many thought that only their keyworker could access their personal data, whereas for databases such as Inform staff can access details on any client of the organisation they work for. Consent documentation could address this misconception.

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This principle is unlikely to apply to homelessness services in their day to day operations. However, in the development of a data set this may be more relevant.

The simplest way to ensure compliance is through anonymisation of the data so that individuals cannot be identified and thus the Act no longer applies.²¹

3.3 OTHER REQUIREMENTS FOR ORGANISATIONS

Homelessness services that collect and record data from their clients need to comply with the Act. There are a number of requirements which arise from this, which are largely mentioned in the section above. There are a few requirements which are worth addressing separately and these are included below. This list is not exhaustive and should not be used in place of checking requirements directly with the Information Commissioner's Office.

Notification

Organisations who need to comply with the Act usually need to notify the Information Commissioner and have basic details of their data processing activities included on their register. There are some exemptions, the most obvious being that those organisations who do not use computers to process information do not need to notify. More details of the notification process and exemptions from it can be found on the ICO website.

Privacy notices

It is a requirement of the Act that information is provided to the individuals concerned in the form of an oral or written statement called a privacy notice. Privacy notices (also known as “fair processing notices”) are in effect the consent documents currently in use across the homelessness sector. The Information Commissioner's Office has a specific Privacy Notices Code of Practice available. In essence, the privacy notice needs to cover:

- the identity of the organisation collecting the information
- what the information is used for
- the consequences for the client of providing or not providing the information

Transparency is central here and the Guide suggests looking closely at what extra information may need to be provided to enable the organisation to process the information fairly and to ensure the individuals whose data is collected are clear about what happens to their data and how it will be used.²²

Subject access request

One of the main rights for individuals under the Act is the right to access their personal data. Organisations are required to respond to any subject access request, to confirm if they are processing personal data of the subject and to provide them with a copy. Within this there are certain exemptions, depending on the circumstances in which an organisation is processing data. Homelessness services will be familiar with withholding third party correspondence from a client who wishes to access their information. There is also provision for exempting some sensitive data such as information about a person's mental or physical health. In most instances an organisation will need to respond to a subject access request within 40 calendar days. In documentation provided by partner organisations for the Critical Mass project approximately half included details about subject access requests in their written statements.

Challenges for services

The DPA presents a challenge to homelessness services particularly in terms of communicating the rights and responsibilities to frontline staff and clients.

Understandably, the Act seems onerous and overly complex. As seen in Section 2.2 'Policy and Procedures' there are different approaches to informing staff of their duties under the Act, with some organisations formally including the key principles of the Act in their policy, whilst others briefly reference the Act. For practical application in frontline services there is a need to instil the principles and themes of the Act as they relate to work with clients and present this to both staff and clients in a user friendly way.

4 CONSULTATIONS

4.1 CLIENT CONSULTATIONS

We undertook a series of client focus groups in order to understand the client experience of the consent to data collection process and understandings of what happens to their personal information. We also wanted direct guidance on how to improve these processes.

Four focus groups were held between 4 November 2010 and 14 January 2011 with a total of 29 client participants, being 22 males and 7 females. All participants were either currently or previously clients of hostels or day centres. One group was held in a day centre with clients from accommodation based services or other support services, two groups were held in an accommodation based services and included clients of other accommodation services run by the same organisation. One group was comprised of Homeless Link's Expert Advisors Panel. Two groups were conducted in London, one group in West Sussex, and one group in South Yorkshire.

Clients were invited to participate in the focus group by their accommodation or support service on the basis that they had current or previous experience of hostels or day centres.

Questions and responses were organised around four themes:

- Permission
- Details
- Use of Information
- Good Practice

The themes were set to explore issues of granting consent around personal data processing and data management from a client perspective.

The research project and the limits of confidentiality were explained at the start of each group. Each participant signed a consent form noting they had been told about the nature, scope and purpose of the research and that notes would be taken during the discussion. The participants were given the opportunity to approach the facilitators individually should they wish to discuss anything in private at the end of the group. No client took this opportunity. The participants were given supermarket vouchers at the end of the focus group, and refreshments were provided.

4.1.1 ACCESS AND IMPARTIALITY:

All the participants in the focus group were selected by the service providers on the basis that they had experience of the support issues being researched. The selection process has implications on the data collected and as such, although not a wholly

representative sample, it does provide a snapshot of individual experiences of consent and data collection.

4.1.2 CONSENT AND CONFIDENTIALITY:

The purpose of the focus group and the research project was explained to participants. Participants were offered conditional confidentiality, meaning that their opinions and comments would be reported without identifying them individually as the source, but any information which indicated the participant or another person was at risk could not be confidential. Participants signed consent forms indicating they understood the purpose and uses of the research. Participants were advised that any comments they made and opinions expressed would not be attributed to them or identified by the location of the session. Therefore, none of the opinions, comments and quotes reported here is attributed to the speaker or the service or location where they were expressed.

4.1.3 RESPONSES

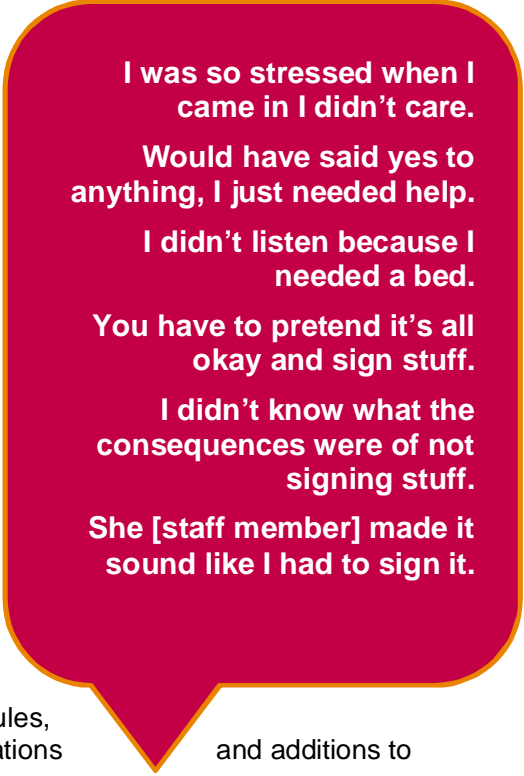
A. PERMISSION:

In this section we asked participants about their experiences of giving permission to homelessness services, such as hostels or days centres, to record their personal data. The question was as open as possible in order to elicit by what different processes permission might have been sought and given, how memorable the process was, what their concerns were and what information they received at the time.

Discussion question:

- When you were first booked into a hostel or started using a day centre did you agree for them to write down and store information about you?

The most common experience, stated across all focus groups, was that clients had been too emotionally distressed and/or physically uncomfortable (through tiredness and/or hunger) to understand or care about giving consent for services to record and process information about them. The consent process invariably took place as part of the process of booking a client into an accommodation based project or day centre for the first time. The booking in process for a hostel generally entails a large amount of paperwork, such as housing benefit and other welfare forms, signing the licence agreement (the tenancy agreement used in hostels), health and safety information, house rules, support agreements and any number of local variations and additions to this.



I was so stressed when I came in I didn't care.
Would have said yes to anything, I just needed help.
I didn't listen because I needed a bed.
You have to pretend it's all okay and sign stuff.
I didn't know what the consequences were of not signing stuff.
She [staff member] made it sound like I had to sign it.

and additions to

All groups stated that at the time they were too worried that if they did not agree to anything being asked of them that they would lose the service or bed space being offered to them. A selection of comments from all groups is included in the break-out box to the right to show the remarkable similarity of participants' experiences.

Many clients did recall signing a consent form, which specifically asked with whom their service could share information. Of these, many cited that they had been provided with a list of different organisations that the service might have contact with and they had selected those with which they agreed to share information. Several participants remembered having discussions with service staff about recording information about them. Few participants volunteered details about giving express permission to the organisation to take down and store their personal information.

There was a reasonably even split across the participants in terms of feeling quite concerned about their personal information or feeling quite confident that the organisation was looking after this information. In one group two participants were quite clear that confidentiality was “a given” and something that they had a right to expect. There was one direct mention by a participant of the Data Protection Act and a working understanding that the Act afforded him rights about his personal information.

It is worth considering the ‘right to expect’ in view of the Data Protection Act; in the first principle of the Act is guidance that the organisations put themselves in the position of the client and thus manage data in ways the client would reasonably expect.²³ (Please see section 3.2 Core Principles of the Act for more detail). With transparency being the watchword of this principle it is clear that the way confidentiality is managed by the organisation needs to be explained explicitly to the client. The concept of confidentiality was very important to all participants and is addressed in greater detail in Use of Information below.

One client raised the point that if first contact with services was through an outreach service (whereby staff actively seek contact with people who are rough sleeping) then there is no equivalent consent process. An ‘on the street’ contact is considerably less formalised than the booking in process to a hostel, but there may still be personal information given to the outreach worker without a process of granting consent or transparency for the client. Another client commented that when he gave permission to share information with other organisations it was filled in on a computer and thus he didn’t sign it, but was offered a print out of the document.

Overall, the level of distress being experienced at the booking in stage with a service cancelled out much of the clients’ ability to take in information and thus make an informed choice about consent to the processing of and sharing of personal information. Clients generally had a better recall of giving permission to share information with other organisations than they did of giving the organisation permission to record, process and store their personal information. There was a general expectation of confidentiality but limited specific knowledge of what this meant in practical terms.

B. DETAILS:

We asked participants about what kind of details they understood were recorded about them and how this information is physically managed.

Discussion questions:

- What information do you think was / is recorded about you?
- Where do you think this information is kept?

Participants provided detailed lists of the types of information they thought were recorded about them. This can be divided into information that was factual and information that was determined/observed about them. The combined list from all the

focus groups of the types of information they thought organisations record included information about: ethnicity, substance use issues, benefits and entitlements, offending history, medical information, next of kin, sexual orientation, challenging behaviour, mental health issues, challenging behaviour, self care, conflicts with staff, problems with neighbours, any “shady” behaviour, and risk information (in the homelessness sector ‘risk’ information usually refers to an assessment of a client’s potential to harm themselves or others).

There was a strong sense of disempowerment in responses to this question. There were a number of responses that indicated clients were not pleased about the information recorded about them. One participant stated he “Dread[ed] to think” what was recorded about him, another replied that he thought staff recorded a “lot of assumptions about me”. There were other comments in a similar vein, about staff recording “hearsay”, things staff had overheard, or “everything”. One participant expressed concern that clients hold back information about themselves because they did not want it recorded and possibly misinterpreted.

Interestingly, participants generally described a significant amount of what could be classified as ‘negative’ information being recorded about them. No participant suggested that staff recorded information about their successes or strengths.



**It all feels a bit
Big Brothery**

There was not significant concern from clients about the way in which their information was stored. Most participants assumed a hard copy file and/or computer were used. There was some limited anxiety about security of information, particularly on computer, mostly related to coverage in the media of laptops or other devices containing personal information being lost. Overall the low interest in how their personal information was secured may be the result of feeling unable to change this or have any say in the process, rather than indicating trust in the process and systems.

One participant stated that he thought that there was a link between what a service received funding for and what they asked him about, and thus what was recorded about him. In one group there was some discussion around the different databases held by different projects and agencies meant that information kept about an individual could be very different, in terms of what the client revealed and what the service chose to record. One client suggested the government may also have a database that held information about them.

Overall clients did not appear to have a clear understanding of what information would be recorded about them by a service and the purpose of such recording. This was especially true of information recorded about them that was not strictly ‘personal factual details’ and might be described as ‘narrative information’.

C. USE OF INFORMATION

We explored client understandings and perceptions of what purposes their information was used for as well as who can access their information.

Discussion questions:

- How do you think this information was / is used?
- Who do you think can see this information?

Participants did not in the main offer that the main use of their personal information would be to help them. Only one participant stated directly that she believed the

information was used “To help us” and in the same group another person suggested the information was used to “Look at your progression” and to assist with move on to the next stage of accommodation. One participant said that the information was used by staff so that they would know how “to treat” her, in the informal rather than clinical sense. From the same group there were further suggestions that personal information would be used to find suitable accommodation, work or training and to carry on a support plan from another agency.

Participants reported very different beliefs about who could see their information, with large inaccuracies at both ends of the spectrum. Some participants thought that only their keyworker and the project manager could see the information recorded about them, whereas others thought funding bodies would have full access to their file. Several participants stated they thought anyone working for the organisation whose service they were engaged with could see their details, and the line was drawn between internal to the organisation (access was open) and external to the organisation (access was closed).


Many participants reported that organisations outside the service may want to see information about them, but they understood that in order for this to happen they would need to provide express permission. Several participants suggested there may be external organisations who may have some right to see their file without the client needing to give permission, such as the police or the Department for Work and Pensions

There was a strong awareness that participants’ personal information would be used in relation to funding processes, to access funding and to report to funders. The level of detail participants thought this would include ranged from anonymous or “relatively anonymous” to funders having full access to their name and date of birth or to all information about them. There was a general sense among participants that their information would in some way contribute to statistics which funders or the government need. Many participants said that if the information was anonymised it was fine to be used for funding and/or statistical purposes. There was some desire expressed for proof that they “really can’t tell it’s me” in any anonymising process and awareness that this meant more than just removing their name, as someone could be identified by details other than their name.

D. GOOD PRACTICE:

In order to best inform our recommendations and toolkit we wanted to get direct advice and guidance from clients about how consent processes and data management could work better.

Participants referred to the first discussion question, where they reported that at initial booking in to a service they were too anxious or physically uncomfortable to understand or care about giving consent to record and process information about them. There was complete consensus in all groups that the consent process needs to happen at a time other than the initial booking in to a service. There was some variation on when this could be done, with answers ranging from the next day to a week, to a month in order to really understand the implications consent.



All the stuff about consent went over my head, could have said they’d poster it around the town and I wouldn’t have heard it on that first day.

of this

Participants asked for more transparency about the uses to which their information is put. Participants suggested that a plain language guide should cover:

- what information is recorded
- who internally has access to it
- who externally has access to it
- some examples of how information is used and for what reasons
- the consequences of giving and declining consent
- details of how to access their own information

It was seen as important that there was a written document as well as a verbal explanation.

On the issue of sharing information externally with other agencies several participants suggested that permission should be sought at each occurrence. There was also a request that staff explain to clients what kind of information needs to be shared and what might need to be, hypothetically, in order that they can better make a decision about this.

Participants who had used day centres pointed out the experience for clients of these services was quite different than in accommodation based services. One participant noted that for many people who have been sleeping rough and/or deeply isolated a day centre is their first contact with a service, or indeed, with other people after isolation, and as such this is an extremely fraught time. Participants asked if day centres needed so much information about people using their services, or if there could be a system whereby the amount of information required could be related to the level of support sought. For example, if only looking for a meal or a shower perhaps this could be first name only, but if further assistance was requested then more personal details would be needed.

At this stage of the focus groups many clients began to ask questions about their personal information. The questions raised included:

- How long is my information kept?
- After I leave the service, who can see my file?
- How is my information destroyed?



One client was very clear that homelessness services should take best practice guidance from the police. The participant cited arrest procedures as clearly explaining a process and the individual's rights. Here the themes are transparency, clarity, consistency and a statement of personal rights.

E. SUMMARY OF CLIENTS' GOOD PRACTICE SUGGESTIONS

The suggestions received from clients on how to improve practice and what they need in order to understand the multiple issues about what happens to their personal information were highly relevant and could be implemented with relative ease.

The four key suggestions were:

- Consent to record and share personal data should not be obtained at the initial booking in process to a hostel.
- Services to provide a plain language guide to what happens to personal information
- Services also provide a verbal explanation of what happens to personal information

- Services need to have different degrees of personal information required and consent processes based on the level of support being accessed by the client.

4.2 PARTNER CONSULTATION

On 20 October 2010 four partners in the Critical Mass project attended a meeting at Homeless Link and participated in a discussion session about their consent and data management policy and procedures.

Questions and responses were organised around three themes and sought to explore how managers understood the data collection and management processes in terms of both their staff and their clients:

- Non-operational use of data
- Communication, understanding and confidence
- Implementation

4.2.1 RESPONSES

A. NON-OPERATIONAL USE OF DATA

We asked the partners about their non-operational uses of client data and two points were discussed:

- Use of data for funding applications / monitoring processes / research – is your consent procedure robust enough for this?
- Do clients know and understand the broader use of their data, even if anonymised?

The partners felt that on the whole they do not make consent explicit around using data for research or funding/monitoring. Using data anonymously without consent is an ethical issue, but it was not clear to the partners whether it was a legal issue. Anonymous data is not of concern to the DPA, and the processing of personal data to make it anonymous for purposes that are

The partners explained that sometimes verbal consent still has to be used depending on the client or the circumstances. The use of verbal consent was thought to be less than ideal; however there are service types and client groups for whom it is a better option. Verbal consent can be a part of a robust consent procedure if carefully managed.

B. COMMUNICATION, UNDERSTANDING AND CONFIDENCE

There were two discussion points around the staff experience of consent and data uses:

- How do you communicate to staff the consent, data protection and confidentiality policy and procedures?
- Do staff understand the uses to which data is put?

Most services said they include information on consent, data protection, and confidentiality policies and procedures in inductions for new staff. Information is also in an Operations Manual, and provided via training.

The partners noted that there is a feeling that staff commonly see data collection as a burden and additional to their support work or lessened their time to provide support to clients which they saw as the core of their role.

Partners also explained that systems need to be flexible to cater for non-office based staff, such as in outreach or floating support situations. Day centres also commented that the time consuming process of consent used in accommodation based services was not viable in their services.

The partners were asked about their perceptions of the clients' experience around the management of their personal information. Three discussion points were raised:

- How do staff communicate to clients how personal data is recorded, kept and shared?
- Do you have concerns about client understanding of consent and making an informed choice? If yes, what would improve this? If no, what practice is working well?
- Do your clients have confidence in the consent and confidentiality processes?

One partner commented that clients seem confident in the consent processes due to their trust in the organisation. It would stand to reason that if the client does not have basic faith in the organisation's general performance then they will not have trust in specific processes, particularly around highly sensitive matters. Overall, there was a sense that clients were more distrustful of, and perceived a higher risk of breaches of confidentiality, with computerised systems than with paper-based systems.

C. IMPLEMENTATION

The partners were asked about how client consent around personal data used is implemented by staff and/or the organisation. There were three discussion points around information sharing, security of information and consistency between staff.

- Do staff check consent is in place before sharing information or recording certain details?
- Is information kept physically secure, online or in hard-copy format?
- How do you manage the inevitable breaches of confidentiality (especially oral / aural)?
- Is there inconsistency between staff results in obtaining consent?

The partners fed back that they thought many frontline staff do not routinely check the specificities of an individual client's consent before sharing information with other organisations. There were inconsistencies between staff in obtaining consent from clients, however it was thought that the staff who were most informed about data practices and able to communicate this to clients received more refusals of consent than staff who offered only limited information to clients.

Breaches of confidentiality were identified as a challenge and can depend on the individual skill of project managers. The physical environment of the service also contributed to the ease with which confidentiality could be maintained – for example, in smaller projects the constraints of the space meant private telephone calls or discussions were difficult to achieve.

The partners also raised concerns about management of access to services when a client refused or withdrew consent to record personal data. Following the discussion

the partners requested that guidance on different levels and methods of consent and managing refusal and withdrawal of consent by clients would be useful.

5 PRACTICE IN OTHER SECTORS

This section looks at practice in other sectors on a range of related issues, including informed consent, practice for frontline staff obtaining consent and recording data, and established practice in research environments. The examples were chosen on the basis of reasonable comparison to homelessness services in terms of working with clients' very sensitive personal information in settings which may be emotionally charged or stressful. In general, we looked at well-developed systems in order to identify what practices that may be applicable to and replicable in homelessness services.

5.1 NATIONAL TREATMENT AGENCY FOR SUBSTANCE MISUSE

There are many similarities between the work of the National Treatment Agency for Substance Misuse (NTA) and homelessness services, in terms of the pressures on and support needs of clients and the resulting confidentiality and personal information issues which need to be addressed. The NTA has a very sophisticated central system of data collection and analyses, but does not impose absolute rules for managing confidentiality and consent issues in the frontline collection of these data.

There are many similarities between the work of the National Treatment Agency for Substance Misuse (NTA) and homelessness services, in terms of the pressures on and support needs of clients and the resulting confidentiality and personal information issues which need to be addressed.

Collecting client data for the NTA presents interesting challenges as the frontline work with clients is conducted by more than 1500 providers across the country. The services provide a wide variety of different types of drug treatment services and thus have different levels of engagement with clients, from community based advice and information through to residential rehabilitation programmes. Providers of specialist drug and alcohol treatment services are obligated to provide a basic level of information to the National Drug Treatment Monitoring System (NDTMS).²⁴

Data are collected in a variety of ways by the providers, however each provider will collect individual data during triage assessment with each patient. This includes things like drugs used and housing needs. Once a month, the data is submitted to regional NDTMS teams who then send it to the central team. The submission of data can be by several methods, from clinical information systems to a web based data entry tool.²⁵

The need of the NTA to respect the right of individual providers to work in ways appropriate to their service type and client needs is balanced against ensuring reasonable consistency in the way the data collection processes are communicated to clients, consent processes, and policy and procedures for staff. This is managed through the provision of guidance documents and toolkits which allow frontline services to develop methods of working that are appropriate to their need and meet NTA obligations.²⁶

CONFIDENTIALITY AND INFORMATION SHARING IN FRONTLINE DRUG AND ALCOHOL SERVICES

For the purposes of this report we looked at a range of documents on confidentiality and information sharing created by the NTA for use by frontline drug and alcohol treatment services. These documents were a briefing on developing policy on confidentiality and information sharing, a briefing on data protection and record retention, guidance the NDTMS data set and a confidentiality toolkit. Here we have focussed on the guidance on developing drug service policies on confidentiality and information sharing in order to understand the legal and ethical concerns of the NTA in the frontline setting, where operational data that later becomes a national data set, is collected.

The briefing document on developing policy on confidentiality and information sharing covers a range of issues that need to be considered by the drug treatment service in determining their specific policy and procedures. Issues covered include confidentiality, information sharing, confidentiality and quality, confidentiality and the law (including breaches), confidentiality and potentially violent or abusive service users, consent, employment practice, children and young people, specific groups and specific settings.²⁷ We have selected particular points of guidance that are interesting and relevant to practice in homelessness services.

The limitations of client confidentiality are addressed in the first section, in that no drug service can offer total confidentiality. The central guidance is that service users understand:

- when information will be kept confidential
- when information will be shared
- under what circumstances there may be legal obligations to breach confidentiality²⁸

The nature of the service provided by many drug treatment agencies requires sharing information with other services in order to provide a seamless treatment journey for the client. There are high levels of multi-agency and cross-sector working in this field. This is similar to homelessness services, who are often in the position of co-ordinating a range of different support for clients, or in assisting clients to gain access to specific support. Again, informed consent is the central issue. The NTA also emphasises that disclosures should be kept to the minimum necessary to meet the objective and only on a 'need to know' basis. Safeguarding procedures to protect client confidentiality are also highlighted, such as determining a way to check the identity of telephone callers seeking information and prevention of unauthorised access to computer based records.²⁹

As in homelessness services, a small number of clients of drug treatment services may at times present with highly challenging behaviour that presents a risk to staff. The NTA guidance states that there is no ethical matter arising in the factual recording of any need for particular precautions in a client's records, including care plans or other information systems. The NTA cites the Department of Health's code of practice information sharing with regard to potentially violent clients; which includes advice that information should always be in writing, except in an emergency; two workers should sign this written information and one should be a manager; the information should be shared with the service user and they have a right to add comments and receive a written copy of information passed between agencies.³⁰

This practice represents a more open way of advising other services of potential risks that may not be seen in homelessness services. Whilst the risk information is generally shared on referral, the client is not likely to be informed of this or shown what has been written. There may be an opportunity for homelessness services to improve practice in this area and it may also present an opportunity to support a client to change their behaviour.

The NTA is very clear on the need for explicit informed consent from the service user in the provision of any personal information due to the highly sensitive nature of the information shared with service providers. Of interest to homelessness services is the guidance that a general information release form, with non-specific advice for clients, such as the “release of any relevant information,” is inconsistent with the principle of informed consent. Services, therefore, need to develop consent forms and procedures which provide specific information relevant to the service on all aspects of what may or will happen to a client’s personal information.³¹

INFORMED CONSENT

The NTA also recommends that employment contracts should include a “duty of confidence” clause that requires staff to adhere to the organisation’s confidentiality policy, including not disclosing any information about service users, the service, staff, management or volunteers without obtaining permission. The contract should also be clear on what disciplinary action may be taken against staff that breach confidentiality policy.

The guidance also notes that some groups of service users may have particular concerns about their confidentiality. This would be similar to experiences in homelessness services, where individuals with blood borne viruses (e.g. HIV or Hepatitis C), or identifying as gay, lesbian or transgendered, or from specific minority ethnic groups for instance may have greater concerns about stigma, prejudice or discrimination as a result of breach of confidentiality. Whilst such groups or individuals have the same rights as other service users they may require more reassurance and support about confidentiality and information sharing practices.³²

LEVELS OF CONSENT IN DIFFERENT SETTINGS

There is provision in the guidance for different levels of consent in different settings. Whilst at one end of the spectrum there are drug treatment workers in prisons who have legal obligations to breach confidentiality where there is a risk to prison security, there are also “low threshold” settings where a client may access services anonymously. In such instances the guidance suggests taking some personal details, but that access to the service is the primary driving force (e.g. in outreach or needle exchanges). Where clients do maintain their anonymity it is still suggested that some information is provided on confidentiality, potentially in writing. If the client starts to disclose personal information or engage in a formal assessment then the parameters of confidentiality need to be explained so that if the client continues to reveal information about themselves, they do so with informed consent.³³

The acknowledgment of different “thresholds” in services and thus potentially different needs in obtaining informed consent is relevant to the many levels of service provision in the homelessness sector. Where there is very low intensity support in particular day centres or drop-ins; or very intensive support in many accommodation based services, there is reason to devise policy and procedures locally that reflect these environments and the needs of the client group.

CLIENT ANONYMITY AND NATIONAL DATA

The detailed guidance on confidentiality and consent practices at the frontline services is a part of ensuring the data received by the NDTMS is submitted with the informed consent of the client. The client records which are reported to the NDTMS have the client's initials and date of birth, which is then automatically turned into a code. Other fields may also be suppressed in order to prevent the very small possibility of 'deductive disclosure' – that information from several sources might be combined to identify an individual. In order to meet the requirements of the DPA the raw data is not available publicly. The NDTMS has several levels of access to its data, with some statistical information available on their website, through to restricted access data to which a researcher must apply for access. The policy of the NDTMS is not to allow service providers access to the raw data (except from their own services) as a further way of protecting service users.

For homelessness services there are opportunities to improve policy and procedures, based on the experience of the NTA and NDTMS. As the homelessness sector moves closer to a national data set drawn from operational data, the NTA and NDTMS are ideal analogues for bridging the gap between frontline services' data collection purposes and national research purposes.

5.2 DEPARTMENT FOR WORK AND PENSIONS

The Department for Work and Pensions (DWP) is responsible for the policy and legislation for welfare and pensions. The DWP has a massive customer base, serving over 20 million customers at any one time. Any exploration of the DWP's data management processes would be a large study in its own right. We know that the DWP does use its operational data to produce research documents and statistics, some of which are published at regular intervals and are available online. In this section we have chosen to focus on how the DWP makes these uses of operational data known to clients. The DWP documents we used for this purpose are top line documents which address their key customer personal information issues.

Comparisons can be made between the experiences of clients accessing homelessness services and customers accessing DWP services. There is a significant power difference between the service and the individual in both cases, where the individual comes to the service in need and has to meet certain requirements in order to receive support. In such contexts consent to use personal information may be seen as a requirement rather than a choice.

Comparisons can be made between the experiences of clients accessing homelessness services and customers accessing DWP services. There is a significant power difference between the service and the individual in both cases, where the individual comes to the service in need and has to meet certain requirements in order to receive support.

THE DWP'S CUSTOMER AND INFORMATION CHARTERS

The first document which customers are likely to access that mentions personal information rights is the DWP's 'Our Customer Charter'. This is simple one-side document which outlines the commitments of the DWP to its customers, the main points are related to the way customers are treated by staff, customer confidence in decisions made by the DWP, timely management of cases and easy access in contact and other services that may assist. The Customer Charter also has four requests of its customers and four further commitments from the DWP, including to "protect your personal information – our Information Charter tells you how".³⁴

The Customer Charter does not provide information on where to find or how to obtain the Information Charter. An experienced internet user can locate it with relative ease, but it is placed on the DWP website under “Customer delivery” which may be interpreted as having a corporate focus, rather than customer focus.

The DWP’s Information Charter is a basic summary of their responsibilities to the customer under the Data Protection Act. The Information Charter states that the DWP needs to collect and “handle” information about customers so that they can provide services. In this process the DWP says that it will ensure that they keep the information secure and “look after” it.

The Information Charter lists a range of responsibilities, briefly and in straightforward terms, on: transparency in the reasons why they need particular information; collecting relevant and not excessive information; securing information from those that should not see it; keeping information no longer than “necessary”; and not making information available for commercial purposes without the customer’s permission. It is interesting that the point on the DWP’s responsibility to *tell* customers when they are sharing information with other organisations is when this sharing is to “give you better public services”³⁵ It may be assumed that there are other reasons to share a customer’s personal information that are not related to giving “better public services” of which the DWP does not, therefore, have to advise the customer.

The Information Charter then refers the customer to a further document – the DWP and Your Personal Information. If accessed online the two documents are linked. The Information Charter states that more detail on the following issues can be found there: finding out what information the DWP has about a customer, how to ask to mistakes corrected, how the DWP ensures information is current and correct, and how to complain. There is also an extended point on sharing information:

... we have [agreements] with other organisations for sharing information and circumstances where we can pass on your personal information without telling you, for example to prevent and detect crime or to produce anonymised statistics³⁶

This point puts several quite important issues together; that the DWP will share your information without consent and then provides two very different examples. Detecting crime does not have a relationship with anonymised statistics, except that the DWP does not tell customers about either activity.

Both charters are very vague and generalised and apply to a broad range of DWP customers. As a result the customer needs to continue accessing other documents in order to get more detail on what the DWP does with personal information. At the third document in the chain, ‘DWP and Your Personal Information’, there is greater detail but it is still a document that clearly needs to cover a very broad range of customers who are accessing the DWP for very different reasons. For example, the opening paragraph ‘Why we collect personal information’ states that the DWP does this for the purposes of:

... social security (including Housing Benefit and Council Tax Benefit), child support, vaccine damage, employment and training, the Financial Assistance Scheme, promoting financial planning for retirement, and policy relating to occupational and personal pension schemes.³⁷

Whilst the legal requirements in managing data are the same for all groups there may be identification differences between a DWP customer needing job seeker's allowance and a customer making a claim for a vaccine damage payment that could affect the interpretation of the document.³⁸

PERSONAL DATA AND RESEARCH

In 'DWP and Your Personal Information' there are three references to the use of personal data for research purposes. The first is in the introductory paragraph where the last line is "We may also use information about you to carry out research about how effective our services are."³⁹ This seems a very limited research remit for the DWP.

The second reference is towards the end of the section 'Information we get or give to other organisations'. This section gives examples of what types of information, reasons for and which agencies and organisations the DWP receives and/or gives information. For a more detailed list customers are referred to a further document.⁴⁰

Customer's personal information may be provided to other organisations for 'research or statistical purposes' carried out on behalf of the DWP and for the external organisation's own research purposes. Here the DWP advises that under these circumstances they will not give out information which could identify an individual.⁴¹

The final research reference in this document is in the section on the Work and Pensions Longitudinal Study (WPLS). Again, the stated purpose of this research is so that the DWP can evaluate its services. There is also the statement that the WPLS is also 'used for a number of limited operational purposes'.⁴² There is a noticeable shift in the complexity of the language here as compared to the previous documents and most of this document. The word 'longitudinal' is quite technical, as is the concept of 'operational purposes' but neither is defined in this document.

ACCESS TO INFORMATION ON PERSONAL DATA MANAGEMENT

The DWP largely directs customers to commence their contact via telephone or online systems, where consent is thus a verbal or 'tick-box' process. Depending on the type of benefit received many customers will continue to have a relatively remote relationship with the DWP that is conducted over the telephone or internet. A customer would have to be actively seeking a greater level of detail in order to obtain further information or documents about what happens to their personal information.

Homelessness services may prefer to provide all their client personal information details in one package, which could include a variety of levels of complexity. As discussed in section 4.1 Client Consultations, service users want this information and also want the issues to be discussed with them.

5.3 HUMAN TISSUE BIOBANK

Data ethics is, understandably, a major issue for the NHS, which has numerous general guidance and codes of practice, as well as detailed policy and procedures for management of confidentiality and patient information in specific contexts. One such example is the Biobank at the Royal Brompton and Harefield NHS Foundation Trust (RBHT).

Homeless Link interviewed the Human Tissue Governance Manager at the RBHT on the broad themes of this report in relation to their newly established Biobank. The

discussion covered the legal and ethical framework for the Biobank and associated consent issues and research ethics.⁴³

The RBHT recently established a research Biobank. Patients undergoing treatment at the RBHT may consent to donation of human tissue samples which will be collected, processed and stored by the Biobank.⁴⁴

The Biobank was selected as reasonably analogous to the homelessness sector as it includes highly sensitive information, and that consent may be required at time that is stressful for the client. Further parallels may be drawn around the client's need for a service and where the consent is to activities that are in addition to the service need. For example, in homelessness services clients are there to access accommodation and other types of support, and the consent to use their information for research purposes is in addition and not directly related to the original needs of the client. The creation of a research dataset in the form of the Biobank was of particular interest in terms of the ethical oversight and management.

In September 2006 the Human Tissue Act (HT Act) came fully into effect. The HT Act defines the law about the removal, storage and disposal of human tissue for public display and health related purposes, such as research. These purposes are referred to as "scheduled purposes". The HT Act defines the range of biological material it applies to, termed "relevant material". Broadly speaking, this is any biological material that contains a human cell or is made of human cells.⁴⁵

The main functions of the HT Act are to:

- define the legal requirement for 'appropriate consent' to remove, store and use human tissue for scheduled purposes
- introduce licensing of premises in which such activities can be carried out
- established the Human Tissue Authority (HTA) as a regulatory body
- set out offences and penalties for breaching the requirements.⁴⁶

The first part of the process of establishing the Biobank was to apply for a licence from the NHS's National Research Ethics Service (NRES). The NRES provides ethical guidance and licensing through independent Research Ethics Committees (RECs). A detailed application is made to the NRES which is reviewed by a REC. The application includes a named licence holder at the RBHT who performs a function similar to that of a data controller under the Data Protection Act and is held responsible for any breaches of the HT Act and the ethical guidance as defined by the NRES licence.

The ethical approval licence lasts for five years and at the end of the period an extension can be applied for or a project completion process is undertaken. The licence holder is also required to report annually to the NRES about research activities and practices.

By having the Biobank licensed the RBHT does not need to apply for ethical oversight for each individual research project as long as the project and the researchers comply with the guidance and parameters of the licence granted. In order to use the Biobank's resources researchers need to apply to the RBHT's Access Committee for approval of their project.

The Biobank samples are held in linked anonymised form. There is a 'link worker' who is able to access the original medical records related to the samples held by the Biobank. This allows the Biobank to facilitate research that they cannot envisage. For example, a researcher requires a set of samples from patients with a particular

history and this exact piece of information is not included with the sample, the link worker is able to look at the medical records and create a sample set. The worker has a code of practice to adhere to and the researcher never has access to the medical records or any personally identifying information.

CONSENT

As with the DPA, the fundamental principle of the HT Act is consent. This must be a positive process whereby the patient actively gives consent. Implied consent or lack of comment cannot be interpreted as a positive process and are thus not valid. The HT Act defines a hierarchy of relationships to the patient of people who can give consent if the patient is unable or incapable.⁴⁷

As with the DPA, the fundamental principle of the Human Tissue Act is consent. This must be a positive process whereby the patient actively gives consent. Implied consent or lack of comment cannot be interpreted as a positive process and are thus not valid.

Currently consent for samples to be stored in the Biobank is taken as a part of consent to a medical procedure, including surgery. The Human Tissue Governance Manager is proposing separating the consent to keep tissue samples in the Biobank from consent to a medical procedure. In the future the consent for retaining tissue samples in the Biobank will be conducted at the initial clinical contact. Patients may have multiple initial contacts, based on time since last treatment of a particular condition, or the presentation of a new condition. Consent would be sought at each of these contacts. This would allow the patient to decide if they will contribute to the Biobank at a time when they are likely to be less preoccupied than when consenting to surgery.

As per the NTA, the insistence on positive consent by the Biobank is a practice that could be formally adopted by homelessness services. The consideration of the timing of the consent process in order to improve the patient's capability to make an informed choice is also a matter that homelessness services can address and where local solutions would be appropriate.

WITHDRAWAL OF CONSENT

There are occasions when patients have consented to the retention of their tissue for the Biobank, but have changed their minds. In such instances the sample is removed from the Biobank and destroyed. If there are also samples from the same patient from other clinical contacts these are also removed, even though these samples still have consent attached. Samples that have already been released to researchers are not sought and any research already completed is exempt as it may not be possible to identify the specific sample or it may void a research project.

This process may be helpful to homelessness services developing policy and procedure around withdrawal of consent and where they will draw the line about what can be removed. This is in terms of defining any client personal information that they do not legally need to maintain and information needed so that the client can use the service.

5.4 RESEARCH BODIES

In the UK there are a number of social research bodies and associations who have already had cause to explore the ethical issues of using sensitive personal information for research purposes. For this report we have looked at the experience,

advice and guidance of the Social Research Association, the UK Data Archive and the Economic and Social Research Council.

The Social Research Association (SRA) is a multi-disciplinary organisation that assists social research practitioners and trainees to network, exchange views and information as well as pursue issues of common concern. The SRA also provides training and information events on a wide range of subjects related to the practice of social research.⁴⁸

The UK Data Archive (UKDA) acquires, curates and facilitates access to the UK's largest digital repository of social and economic data. The UKDA means data that have been collected for one study can be analysed again for a completely different research project. The UKDA also provides best practice guidance and training in managing and sharing research data. The UKDA is based at the University of Essex.⁴⁹

The Economic and Social Research Council (ESRC) is the UK's largest funder of research on economic and social issues. The ESRC supports independent, high quality research which has an impact on business, the public sector and the third sector. At any one time the ESRC is supporting over 4,000 researchers and postgraduate students in both academic and independent research settings. Here we have used their ethics guidance for applicants for research funding.⁵⁰

5.4.1 ETHICAL RESPONSIBILITIES TO SUBJECTS

In their 'Ethical Guidelines' the SRA states that researchers have four key areas of obligation – to society, to funders and employers, to colleagues and to subjects. Of interest to this report are the obligations to research subjects. The SRA states:

Social Researchers must strive to protect subjects from undue harm arising as a consequence of their participation in research. This requires that subjects' participation should be voluntary and as fully informed as possible and no group should be disadvantaged by routinely being excluded from participation.⁵¹

Of course, the subjects supplying personal information to homelessness services do so in the first instance in order to receive support, and the support may be predicated upon having a certain amount of information. Changing use of these data from an operational to a research context needs the fully informed and voluntary consent of the subject – the principle quoted above does not make exceptions for data that are anonymised. However, the principles of the SRA's obligations to subjects can be applied to both the operational and research data needs; indeed, applying the same ethical principles to operational and research data will help to create a transparent and straightforward process for the organisation and the client.

Even when no identifying information is given by the subject to the research, such as in a survey or informal interview, informed verbal consent is advised. Supplying the subject with an information sheet about the research, covering the nature and scope of the research, the identity of the researcher and what will happen to the data that are collected is suggested by the UKDA.⁵²

The SRA is aware that when working with 'vulnerable populations', especially if in a dependent relationship with the researcher, as clients of homelessness services are dependent in their relationship with providers, a limitation on what can be considered informed consent develops. As the homelessness service also has a vested interest

in obtaining consent to use the operational data for research it may be possible to argue that any consent process they institute cannot be informed as their interest will constitute persuasion of the subject.⁵³

The ESRC advises that when seeking consent from vulnerable groups, passive or group assent is not acceptable. Every effort should be made to develop methods of seeking consent that are appropriate to the client group.⁵⁴ In the focus groups we conducted as a part of this research (see section 4.1 Client Consultations) clients were clear about the process and the information they want in order to make a decision about consent.

It is challenging to create an environment in homelessness services where frontline staff are able to give enough information about uses of personal information and not unduly persuade a client into giving consent, and where clients feel that they can refuse some aspects of consent without loss of support needed. It may not be possible to guarantee completely

It may not be possible to guarantee completely informed and voluntary consent, especially in the context of an unequal power relationship, such as between clients and homelessness services, but aspiring to this and adhering to key ethical principles is central to protecting the client from undue harm.

informed and voluntary consent, especially in the context of an unequal power relationship, such as between clients and homelessness services, but aspiring to this and adhering to key ethical principles is central to protecting the client from undue harm.

5.4.2 GOVERNANCE AND ACCESS

As well as ethical guidelines many sectors who conduct research with human subjects also have formal governance in the form of ethics committees. In the NHS, for example, any research conducted with staff or patients must be submitted to local and/or regional committees for ethical approval prior to commencement. A research ethics committee can provide formal checks and safeguards for researchers, subjects and organisations.⁵⁵

The SRA suggests that ethics committees can also maintain ongoing ethical review of research projects. The level of this supervision may vary, but the idea is that it cannot be assumed that all ethical concerns have been resolved at the outset of the project and the aim is to ensure that there is a contingency plan for unanticipated ethical problems.⁵⁶

An 'ethical checklist' can be used to facilitate governance and stimulate ethical considerations throughout a project. The key fields suggested by the SRA are:

- Project title
- Expected duration
- Identity of field researchers and organisational base
- Purpose of study
- Sources of funding
- Scientific background
- Design of the study
- Potential benefits and hazards
- Recruitment procedures

- Informed consent
- Data Protection
- Confidentiality and anonymity
- Monitoring of the research
- Dissemination of findings⁵⁷

These fields include both direct and indirect ethical considerations. Any issue likely to affect the success of the project is of ethical interest as it may expose the subject to risk or exploitation.⁵⁸

Access to data for research purposes is another aspect of managing the ethics of research. There is a balance which needs to be struck between the protection of clients from potential harm and making the data available for a variety of research uses and the new knowledge which can arise as a result.

A data set may be held in a data centre or archive, such as the UK Data Archive, which is not in the public domain but is still available to researchers with certain caveats. Researchers wanting access to data held in this way are required to register with the service and usage of the data can be restricted to specific purposes. Researchers may be asked to agree to an 'End User Licence' which imposes certain conditions on the researcher. Different levels of restriction and conditions can be applied as relevant to the data set.⁵⁹

Research ethics committees can also play a role in access to a data set. They may be involved in determining the specific purposes of data use and the conditions on the user. Alternatively, researchers may need to apply to the ethics committee in with details about the project as per the checklist above in order to gain approval to access the data set. In such instances the UKDA advises that an ethics committee needs to value the principle of data sharing and be looking for ways to do this whilst also protecting the rights of the subjects.⁶⁰

Different levels of restriction to data can be based on the sensitivity of the data and the level of anonymisation applied to the data set. As discussed below (section 6, Practical aspects of anonymisation and data sharing), a lighter touch in anonymisation may provide a richer dataset, but may mean tighter restrictions on access will be needed.

The good practice, guidance and codes of practice of established research bodies have a lot to offer the homelessness sector as we move towards the creation of a national data set. In time, the sector will need its own code of practice and potentially a research ethics committee or similar to provide guidance and oversight on the development and uses of the data set.

6 PRACTICAL ASPECTS OF ANONYMISATION AND SHARING DATA

Of particular interest to this project are the legal and ethical obligations of organisations when anonymising personal data originally collected in an operational context, sharing this data outside the organisation for research purposes and potentially aggregating this data with other data sets.

Whilst the Data Protection Act is only concerned with personally identifiable data it makes clear that subjects need to be informed of all planned and potential uses of

their information. As discussed in section 5.4, social research organisations are also clear that there is a duty to obtain informed consent even when the data is collected anonymously. Consent to use data in this way can easily be woven into the general processes of consent to record personal information. Our research with clients indicated no concerns about this type of use of personal data, as long as individuals could not be identified.

6.1 THE PROCESS OF ANONYMISATION

Whilst at first glance the anonymisation of client data appears simple, closer examination reveals a myriad of issues, and potential issues, which need to be resolved in order to ensure the development of a robust dataset.

REMOVING IDENTIFIERS FROM QUANTITATIVE DATA

The client data used for analysis in Year 1 of Critical Mass was drawn from the Link client recording systems as used by the seven partner organisations. The data was anonymised by technical staff already working with Link before it was made available to the research staff.

To anonymise the data, a number of fields were removed which could be used to identify the client. These included:

- Name and nickname
- Link ID number
- Date of Birth (changed to 1/1/YOB to allow analysis of client ages without compromising anonymity)
- Address/email/phone/fax numbers and previous address and postcode
- National Insurance number
- Disability details (free text fields, some of which contained names of clients)
- Physical description
- Housing benefit reference number
- Service charges and personal service charges
- Next of kin/contact person's name, relationship and contact details
- Rent
- Housing Association name, contact details and codes
- Landlord's name, company, address, contact details
- RSL's contact details and codes
- Means of ID
- Keyworker/lead worker/support worker/case coordinator/named worker/agency worker/associate worker/resettlement or move-on lead – name and project
- Doctor's name, surgery and contact details
- Support hours

However, even with these details removed, the records were still in the same order as found on the Link database. To resolve this potential breach in anonymity, whereby the client could be identified by connecting the position in the record list with the position in the Link database, the lists were twice subjected to randomisation, making any reconnection of record to client by referencing position in list extremely unlikely. A new 5 digit client ID was applied to replace the Link ID numbers after the process of randomisation, numbering them in a monotonic sequence (e.g. 00001, 00002, 00003).

In their general guidance on anonymising data, the UK Data Archive advises:

- Personal data should never be disclosed unless there is explicit consent.
- Define an appropriate or reasonable level of anonymity
- Aim to maintain the maximum level of meaningful information
- Replace identifiers where possible, rather than remove altogether
- Don't over-anonymise – some identifying information may provide valuable context⁶¹

In anonymising quantitative data the UK Data Archive suggests:

- Removal of direct identifiers: name, address, postcode, institution, photograph
- Reduction of the precision or detail of a variable through aggregation: year of birth instead of date of birth, occupational category rather than job title, general locality / area rather than name of village
- Restriction of extreme upper and lower ranges of a variable to hide outliers: age (the very young or very old may stand out)⁶²

REMOVING IDENTIFIERS FROM FREE TEXT AND QUALITATIVE DATA

No free text entries were used for Critical Mass as this level of qualitative information contained very sensitive personal data that could be linked to the client. Whilst there are ways to manage qualitative data of this kind, it was not used for Critical Mass. Even though the free text was removed from the dataset the classification of the entry was kept. In Link much of the inputting of detail about work with a client is entered as a particular action type (e.g. Health - registered client with a GP or Substance Use – client referred to treatment service) and keeping these action types provided a rich level of information even without the free text.

The UK Data Archive also provides general guidance on managing the anonymisation process for qualitative data, such as that obtained in an interview or in free text responses. The main emphasis is on ensuring the quality and depth of the data.

Key points include:

- Avoid blanking out information – use pseudonyms or replacements instead
- Avoid over-anonymising – the removal or aggregation of information in text can distort data, making them unreliable, misleading and potentially unusable.
- Ensure there is consistency of process among the team throughout the project
- Use brackets [xyz] to identify where replacements have been made
- Maintain an 'anonymisation log' of all replacements, removals or aggregations that have been made which must be kept separately to anonymised files.⁶³

MANAGING DUPLICATION OF RECORDS

It is important to have a plan for managing duplications within raw data so that they can be resolved before anonymisation. If duplications are not removed, the potential to create a distorted data set is high. For example, a client may have two separate entries within one organisation resulting from, for example, input errors in spelling of names.

The decision about which field will be used to locate duplicates needs to be carefully thought through. False positives (apparent but not actual duplicates) may result from use of name or date of birth to identify duplications – many people do have the same name, input error misspellings may create same names and many people do have

the same date of birth. For Critical Mass the technical staff used National Insurance Numbers to identify duplications.

6.2 ISSUES TO ADDRESS BEFORE ANONYMISING DATA

As noted above, over-anonymisation can be highly counter-productive and may render the dataset unusable. Even the distortion or lack of context for the data may make the dataset significantly less useful and robust than if the process of anonymisation had had a lighter touch.

One way to avoid over-anonymisation is to define as many research queries as possible before removing personally identifying information. It can be useful to engage a variety of different people from different specialisms within the organisation (and where possible, external input) in imagining what the service would like to know about the clients collectively and a range of questions to ask of the data.

For example, how the location of the client is anonymised can have a dramatic effect on the types of questions that can be asked of the data and what analysis will be possible. The options for how to do this will also be affected by the size of an organisation – a large, multi-site service provider will have options to anonymise location that will not be possible for a single site provider. However, if the data is aggregated with other providers then a single site service will need an anonymisation strategy for the location, ideally a strategy that is common to all contributors to the aggregated dataset. Before removing the location (or other potential identifiers) the service needs to think through what potential analysis they may have for this variable. For example:

- compare client experiences at different locations
- examine the differences in urban and rural services
- look at variations in outcomes in different boroughs

Similar examples include benefit type and amount, previous accommodation, next accommodation, external support services engaged with (eg drug treatment, mental health team) or statutory agencies engaged with (eg probation).

For any variable that does not directly identify a client but could be used to do so, a discussion process looking at the data it provides or could provide, and options other than removal, is recommended. Where maintaining a variable that could potentially be identifying is key to analysis then another option is to impose access restrictions on the data.

6.3 LINKED ANONYMISED DATA

Some services may prefer to hold their data in linked anonymised form. Linked anonymised form is a way to have an anonymised dataset available for research needs, but retain a way to go back to the original unanonymised data in order to make further research queries. For example, a researcher may have a query that cannot be answered by the data in its current form – e.g. they would like to look at the relationship between level of education reached and outcomes for recovery from homelessness. The dataset as it stands does not include information on level of education achieved. With a linked anonymised dataset it is possible to return to the original client files to extract the data on educational levels and add this detail to the anonymised data set.

If the client data is held in linked anonymised form there is need for policy and procedures to define a named link worker who 'holds the key' to linking the

anonymised data with the original client file. The researcher should not be a part of this process and should only ever have access to the anonymised data. There is also a need for policy which defines the circumstances under which the data will be unlocked and protocols to manage the process so that it is ethical and legal.

6.4 LIMITATIONS OF ANONYMISATION

Anonymisation is not a definitive process and there cannot be a 100% guarantee that a client will not be identified. An organisation should not promise absolute anonymity to a subject, but that they will remove key identifying information before releasing the data from the organisation. Frontline homelessness staff should, therefore, have a basic understanding of what identifying information will be removed in order to explain this to a client or to answer queries about the process.

7 CONCLUSIONS AND RECOMMENDATIONS

Our research has shown that the experience of analogous services and social research bodies is that there is a fundamental need for consent for all uses of client data. This does not require significant changes to current practices in homelessness services.

The exploration of current practice in homelessness services around personal data revealed a great deal of variation in the resources provided to staff and clients. At the same time, the general legal requirements were met. However, as the DWP documentation shows, just meeting the general requirements means a lot of pertinent detail is not supplied. As seen in the NTA, there can be good practice achieved in developing policy, procedures and resources for client's personal information management through a toolkit that shows what is necessary, but respects the need for local augmentation.

Unlike the NTA or the DWP, across the homelessness services landscape there is currently no central organisation collecting information, no governing body able to obligate services to collect specific data or provide guidance on policy and procedure. The nearest analogue was the requirement for services who received Supporting People funding to submit certain data centrally (client record forms); however, in April 2011 this requirement was ended.

Guidance and tools on many of the issues discussed here are being developed for homelessness services as a part of this project. Homelessness services are working in the context of the end of the Supporting People centralised data collection, a lack of a central homelessness data collection and the absence of governance that applies to all services. As a result, the variety and detail of data collected, policy and procedures for management of client information and methodologies for analysing data are likely to significantly widen in the future, especially in a political climate emphasising 'localism'. The need for the sector to manage its own larger data set is imperative if homelessness services want a robust and substantial evidence base to influence policy and practice.

Whilst there is a great amount of detail yet to be determined regarding the homelessness sector potentially developing and managing its own centralised national data set, in terms of the ethical and legal issues arising from using operational data in research contexts there will need to be a several sector-wide standardisations and agreements, such as:

- In frontline services, the standardisation of consent practices, policy and procedure as they relate to the use of client personal data in external research
- The adoption of ethical guidelines or a code of practice across all homelessness services contributing data
- The development of a Research Ethics Committee for the sector to advise on data collection, management of raw data, anonymisation, access to the data set, approval of research projects and general ethical oversight.
- Provision of access to the dataset for services and other researchers, potentially through the use of an online data archive (such as the UK Data Archive) as a way to encourage novel research to take place with the data
- Potentially close management of access to the data set, so that data that has been subjected to minimal anonymisation can be held safely and research projects approved prior to access.

There is a wide variety of good practice and replicable models across services that provide support to people in need and established practice in social research that can be drawn upon to put in place strong ethical frameworks for external research uses of client personal information concurrent to the development of the data set.

For the short to medium term, Homeless Link has developed an [Ethics Toolkit](#)⁶⁴ to assist organisations to look at the legal and ethical issues in their management of client personal information as it is currently used, and points to consider for potential future uses of their operational data for research purposes.

Homeless Link
April 2011

Homeless Link, Gateway House, Milverton Street, London SE11 4AP
+44 (0) 20 7840 4430 | info@homelesslink.org.uk | www.homeless.org.uk

Chief Executive: Jenny Edwards | Chair: Ann Skinner | Charity Registration No. 1089173 Company Registration No. 4313826

¹ Supporting People was a funding stream from central government administered by local authorities which specifically funded accommodation based services for homeless people. As a part of this funding stream service providers were required to provide data to a central source. This data can be found at spclientrecord.org.uk The Supporting People funding stream is no longer specifically delineated in local authority budgets and this data collection and analysis ceased in April 2011.

² In-Form is a client information recording database created and managed by Homeless Link. An earlier version of this database was called Link.

³ Homeless Link SNAP 2010

⁴ Feedback from partner agencies received during partners' meeting of 21 July 2010 at Homeless Link.

⁵ Information Commissioner's Office, The Guide to Data Protection, undated but reflects the law as at 1 October 2009, available at http://www.ico.gov.uk/for_organisations/data_protection/the_guide.aspx downloaded 4 November 2010 p. 2 – 5, 31

⁶ Ibid p. 22

⁷ Ibid p. 23

⁸ Ibid p. 25

⁹ Ibid p. 26

¹⁰ Ibid p. 26

¹¹ Ibid p. 37 – 108

¹² Ibid p. 43

¹³ Ibid p. 45

¹⁴ Ibid p. 110

¹⁵ Ibid p. 53 – 54

¹⁶ Ibid p. 57 - 59

¹⁷ Ibid p. 63 – 67

¹⁸ Ibid p. 72 – 73

¹⁹ Ibid p. 81

²⁰ Ibid p. 82 – 83

²¹ Ibid p. 93 – 95

²² Ibid p. 49

²³ Ibid p. 43

²⁴ Homeless Link interview with Brian Eastwood, TOP Implementation Manager, National Treatment Agency, March 2011

²⁵ National Treatment Agency for Substance Misuse 'NDTMS Data Set – Guidance for Drug Treatment Providers' 19 June 2009 Version 5.3.2

²⁶ National Treatment Agency for Substance Misuse 'Developing drug service policies: 1 – Confidentiality and information sharing' September 2003

²⁷ Ibid.

²⁸ Ibid.

²⁹ Ibid.

³⁰ Ibid.

³¹ Ibid.

³² Ibid.

³³ Ibid.

³⁴ Department for Work and Pensions 'Our Customer Charter' undated. See

<http://www.dwp.gov.uk/docs/customer-charter-dwp.pdf> Retrieved 20 January 2011

³⁵ Department for Work and Pensions 'Information Charter' November 2009 See

<http://www.dwp.gov.uk/docs/dwp-information-charter.pdf> Retrieved 20 January 2011

³⁶ Ibid.

³⁷ Department for Work and Pensions 'DWP and your personal information' November 2009 See

<http://www.dwp.gov.uk/docs/dwp-your-personal-information.pdf> retrieved 20 January 2011

³⁸ A vaccine damage payment is a lump sum payment made to people who have become severely disabled as a result of receiving particular types of vaccines in the UK. Customers affected need to apply for this payment within certain time frames.

³⁹ Department for Work and Pensions 'DWP and your personal information' November 2009 See

<http://www.dwp.gov.uk/docs/dwp-your-personal-information.pdf> retrieved 20 January 2011

⁴⁰ Ibid.

⁴¹ Ibid.

⁴² Ibid

⁴³ Homeless Link interview with Clare Dundas, Human Tissue Governance Manager, Royal Brompton & Harefield NHS Foundation Trust, 4 March 2011

⁴⁴ See <http://www.rbht.nhs.uk/research/research-facilities/biobank/>

⁴⁵ See <http://www.rbht.nhs.uk/healthprofessionals/clinical-departments/laboratories/human-tissue-act/>

⁴⁶ Ibid.

⁴⁷ Dundas, C. op cit.

-
- ⁴⁸ See www.the-sra.org.uk
- ⁴⁹ See www.data-archive.ac.uk
- ⁵⁰ See www.esrc.ac.uk
- ⁵¹ Social Research Association 'Ethical guidelines' December 2003, p. 13 - 14 www.the-sra.org.uk/documents/pdfs/ethics03.pdf Retrieved 8 November 2010
- ⁵² UK Data Archive 'Managing and Sharing Data a best practice guide for researchers' University of Essex, 2009 p. 18
- ⁵³ Ibid. p. 30
- ⁵⁴ Economic and Social Research Council 'Framework for Research Ethics' (undated) p. 30
- ⁵⁵ Social Research Association, op cit, p. 41
- ⁵⁶ Ibid. p. 42 - 43
- ⁵⁷ Ibid. p 52 - 55
- ⁵⁸ Ibid. p. 52
- ⁵⁹ UK Data Archive 'Managing and Sharing Data a best practice guide for researchers' University of Essex, 2009 p. 21
- ⁶⁰ Ibid p. 18
- ⁶¹ UK Data Archive, University of Essex 'Research ethics and data confidentiality: anonymisation and access control' Presentation at conference: Managing and Sharing Social Science Research Data: Legal and Ethical Issues, British Library, 8 April 2011
- ⁶² Ibid.
- ⁶³ Ibid.
- ⁶⁴ See <http://homeless.org.uk/toolkits-and-handbooks/critical-mass/ethics-main>