DATA PROTECTION AND CONFIDENTIALITY

Last updated: August 2018

Lawfulness

CQC consider the lawful basis for processing data for the NHS Patient Survey Programme (NPSP), is Article 6(1) (e) of the General Data Protection Regulation (GDPR): '*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*.'

The NPSP includes some special categories of personal data. This is data that under the GDPR is considered more sensate and needs more protection, examples include, ethnicity and sexual orientation. CQC consider the lawful basis for the processing special categories of data is Article 9(2)(h): *'processing is necessary for the purposes of […] the management of health or social care systems and services'.*

When carrying out your survey, you will need to ensure that you comply with the General Data Protection Regulation. You can do this by carefully following the survey instructions as set out in this document, as well as the relevant survey handbook, and instruction manual, as published on the NHS Surveys website.

If you have not already done so, please ensure that you include research in your data protection registration.

You must take steps to inform people using your services that their contact information may be used for the purpose of the NHS Patient Survey Programme that, where relevant, this will include passing those data to an approved contractor, and that they have the right to opt-out of this. One way to do this is to ensure that your privacy notice includes the NPSP.

To meet your obligation to inform people using your services of their right to opt-out, you must continue to put up posters and leaflets during the sampling period and fieldwork; and these must provide people with contact information to opt out of the survey. Any objection to taking part must be respected. Another way to inform people is to publicise the survey locally. Please see the survey instructions on publicising the survey for more information.

GDPR requires personal data to be processed in a manner that ensures its security and must not be processed or accessed unlawfully. You must ensure that all responses are kept confidential.

You will also need to comply with the NHS Code of Practice on Confidentiality (2003), which incorporates the Caldicott Principles. You should take particular care to ensure that your use of patient/service user data complies with these principles. In particular, you should be aware of the flows of patient/service user data, and the issues which these present.

It is your legal responsibility to ensure that you meet any guarantees of anonymity or confidentiality made in covering letters and on the questionnaire.

Working with an approved contractor

It will be necessary to establish appropriate contractual arrangements with any contractor. Your trust's Caldicott Guardian and legal advisors should advise you on these matters. The use of the approved contractor, and the processes for their work on behalf of your trust in the NPSP, should be reviewed and approved by your Caldicott Guardian. We recommend that your Caldicott Guardian should consult your Data Protection Officer prior to approval, so as to obtain their advice on compliance with GDPR.

GDPR places further obligations on data controllers (trusts) to ensure contracts with processors (approved contractors) comply with the GDPR. Processors must be able to provide controllers with 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected.

The Approved Contractors who have been appointed for the NPSP have all been through a competitive procurement process as part of which they provided information about their processes for ensuring the confidentiality and security of personal information. The framework agreement between the approved contractors and the Care Quality Commission contains clauses stating that the approved contractor will comply with the General Data Protection Regulation.

The model service contracts provided by CQC for use between trusts and approved contractors are GDPR compliant. You are advised to check these with your own legal department to ensure that they fulfil your requirements and amend as needed. If you do not use these, you are advised to ensure your own contracts are GDPR complaint.

Guidelines on the use and security of the data collected have been agreed by the Care Quality Commission (CQC) and the Survey Coordination Centre for the NPSP. These guidelines will help to ensure that data are handled in a manner most in keeping with the spirit of the GDPR and the Social Research Association and Market Research Society's *Guidelines for social research* (2005). They have implications for approved contractors and for NHS trusts conducting surveys in-house.

Information about the GDPR can be found at the Information Commissioner's Office (ICO), and the Market Research Society provides further guidance on data protection.

Statements of compliance with data protection (In-house trusts only)

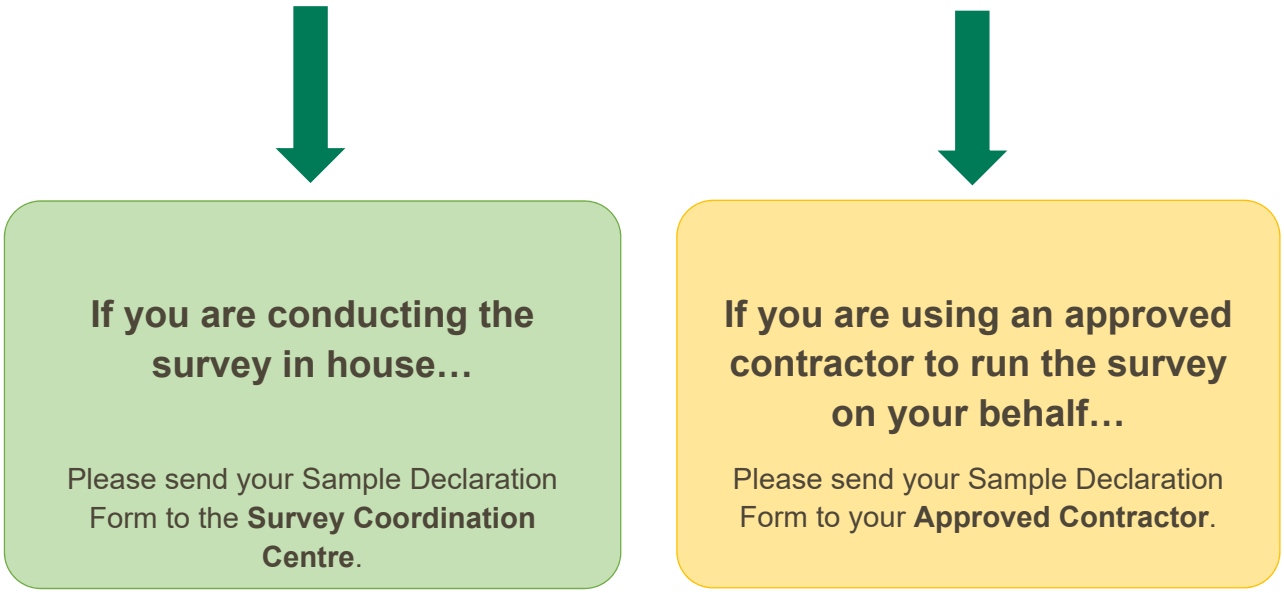
If you are conducting the survey in-house, that is, you are undertaking the survey yourself and have not employed the services of an approved contractor, you must ensure that a Declaration of Compliance with the General Data Protection Regulation is completed for all staff working with the data which must be signed off by your trust's Caldicott Guardian. Only trust staff who have completed this declaration will be authorised to view this restricted data. If the trust's Caldicott Guardian does not authorise this, the trust must carry out the survey using an approved contractor.

This form can be found in the relevant survey folder on the NHS Surveys Website .

Sample Declaration Form

Each NHS trust has a Caldicott Guardian responsible for overseeing the proper use of patient/service user data. Under Section 251 approval, both the Caldicott Guardian and the person drawing the sample must complete their respective sections of the Sample Declaration Form. We recommend that your Caldicott Guardian should consult your Data Protection Officer prior to signing the form, so as to obtain their advice on compliance with GDPR.

The Sample Declaration Form constitutes a legal document whereby the trust authorises the sample to be transferred outside the trust. Sample Declaration Forms are different for each survey and can be found in their respective folders.



Approval under section 251 of the NHS Act 2006

Approval for surveys in the NPSP are sought under **Section 251 of the NHS Act 2006**. This approval allows the common law duty of confidentiality to be put aside in order to enable the processing of patient identifiable information without consent. The survey methods are reviewed by the Health Research Authority (HRA), and the Confidentiality Advisory Group (CAG) of the Health Research Authority grants a recommendation of support. Although the support is for the transfer of names and addresses to contractors, which does not apply to in-house trusts, it is still expected that in-house trusts follow the instructions in full.

Any deviation from the procedures described may lead to breaches in patient confidentiality and could lead to action being taken against an NHS trust.

The recommendation of support does not cover the transfer of patient identifiable information where a patient has indicated **dissent** - by this we mean instances where a patient/service user has explicitly indicated that they do not want their information to be shared for purposes such as patient surveys, or specifically stated that they do not want their details shared outside of the trust. It is strongly advised that trusts follow the same procedures as outlined in the recommendation for support from the CAG.

- Patients/service users who have indicated they want to be excluded from surveys or do not want their address details shared for any reason other than clinical care must be excluded.
- This should be done by referring to your local records.

Processing Opt Outs

Following the requirements of the Section 251 approval for the NPSP, trusts are required to process any opt outs from patients/service users as follows:

1. Any objection is to be recorded immediately and checks made to determine whether a mailing is underway. If a mailing is underway the caller will need to be advised that it might not be possible to prevent this mailing but assured that they will receive no future mailings.
2. People wishing to receive no further questionnaires can be identified with a flag/code/number on the mailing file.
3. When speaking to callers wishing to opt-out of future survey mailings, it is not appropriate to try and dissuade them from their intent. Even a well-intentioned discussion around the benefits of the survey could be perceived as applying pressure to participate. The benefits of the survey should only be mentioned by call-takers in response to queries from callers. If someone feels strongly enough about the survey that they initiate contact to object, this needs to be respected and acted upon immediately to avoid upset and misunderstanding.
4. Callers are advised they are being removed from the mailing list **for this survey only** and that if they wish to register their dissent against wider research participation at their trust, they need

to speak to their trust (via PALS or the trust's Information Governance Team). We expect trusts will have their own systems in place for reflecting this in patient/service user records.

Additionally, you are required to discuss this issue with your Caldicott Guardian to ensure that any patients/service users who have indicated that they do not wish to have their details shared for purposes such as this survey, yet may have sufficient address details visible in PAS, are not included in the sample that is submitted to the Survey Coordination Centre.

Please note that the national data opt-out does not currently apply to the surveys running under the NHS Patient Survey Programme in 2018/19 and you must not exclude people on this basis.

The programme will continue to use the separate opt-out mechanisms described in this document. For further information please see the National Data opt-out operational guidance policy.

Keeping patient mailing data and sample data separate

For patient confidentiality reasons, patient/service user responses must never be matched to the individuals that made them. To do this you must store patient/service users name and address details separately from sample information and survey response data. To comply with data protection principles, you must ensure these are securely stored.

If you are conducting the survey in house…

Once the sample has been returned from DBS and your sample is ready to submit, you need to remove patient names, addresses and postcodes from the sample file to a 'mailing file':

1. First, give each patient/service users a unique number (a Patient Record Number, or PRN). You will use this number to link both files; the mailing file and the sample file. This number must be available and correctly matched on both the mailing file and the sample information file.
2. Second, split your file in two: one file will be the mailing file, and will contain the PRN and all the patient/service user's details necessary for mailing (name, address etc.), the other file will be pseudonymised and will contain the PRN and sample information (gender, year or birth, and so on).
3. You will use the mailing file to deliver the survey via the postal service. **This file must not leave your trust.**
4. You will submit the sample file to the Survey Coordination Centre via a secure FTP.

If you are using an approved contractor…

You should send one single file containing both the mailing data and the sample data to your contractor via their secure method of data transfer. Your contractor will give you instructions on how to submit the data via their secure FTP. After running the required checks, your contractor will separate the mailing and sample data.

Once the contractor has confirmed they have completed their checks you must separate and securely store these files as described above.

You must never send patient identifiable data via email.

This will constitute a breach of the Section 251 approval for the survey and will result in action by the CQC. Your Trust would also have to consider reporting the breach against your Information Governance Toolkit as a 'Serious Incident Requiring Investigation (SIRI).

Encryption of personal data

Any patient identifiable information sent between trusts and contractors must be in an encrypted format with password protection, following the requirements in the box below:

When you send data you must use…

- An encrypted session based on the Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protocol (for example as with HTTPS or SFTP)
- A key size of 256 bits or greater

This will protect against any accidental or intentional interception during the transfer of patients' details.

Mailing questionnaires to patients/service users

The envelope(s) used to mail out your survey materials to patients must not show any indication of the NHS trust name. This is because some patients may not have told family or friends that they have gone to hospital and it is important that this information remains confidential to the patient.

Assurances of patient/service user anonymity

It is important to ensure that any claims you make about patient anonymity are accurate; you are obliged by law to honour any statements that you make.

In most cases it is not accurate to tell patients/service users that their responses will be anonymous: often, the person who receives the completed questionnaires would be capable of matching these responses to patient names and addresses. Instead, you should inform patients that their data are treated confidentially.

Patient/service user confidentiality

Data analysis, and any reporting or publication are also subject to data protection principles. To help ensure this please follow the guidance in this section.

The NPSP includes some special categories of personal data. This is data that under the GDPR is considered more sensate and needs more protection, examples include, ethnicity and sexual orientation. CQC consider the lawful basis for the processing special categories of data is Article 9(2)(h): *'processing is necessary for the purposes of […] the management of health or social care systems and services'.* Personal data processed by the trust and approved contractor (acting under the trust's responsibility) takes place under the professional duty of confidentiality.

It is essential that any patient survey is conducted in such a way that patient confidentiality is respected and given the highest priority. The covering letters that accompany the mailed questionnaires inform patients that their name and address will never be linked to their responses. Furthermore, patients/service users' responses must not be presented to anyone in a way that

allows individuals to be identified. For example, if a patient is known to have stayed on a particular ward and his or her year of birth, sex and ethnic category are known from their survey responses, it might be possible to use this information to identify them. It would be unlawful to provide staff who may have had contact with respondents any information that would allow these respondents to be identified.

The following recommendations are made:

1 The raw data set should not be provided to any member of staff at the trust who does not need to view it (i.e. those who are not directly working on the project).

2 If data are to be presented to other trust staff, only the aggregated totals for each question should be provided. If analysis by subgroup is carried out, the results for any group consisting of **fewer than 30 respondents (or 20 for the Children and Young People Survey) should be suppressed (replaced by a dash)**. The data should be presented as in the example Table 1 below. In this case, responses for the 'Mixed' and 'Asian' ethnic categories are suppressed (though the subgroup totals are shown):

Ethnic category	Were you ever bothered by noise at night from hospital staff?		
	Yes	No	Total responses
	%	%	n
White	81	19	261
Mixed / Multiple	-	-	8
Asian	-	-	18
Black / African / Caribbean	79	21	52
Other	85	15	36

3 Do not present response information (including comments) in a form that allows an individual patient/service user to be identified by the group receiving the information. For example, if you are presenting the results for a small number of individuals, make sure that it will not be possible for the reader/audience to identify individual patients/service users from their responses.

4 Additional information specific to a survey that can be used to identify individual patients/service users must be removed. The sample information collected for each survey varies, please see the relevant survey handbook for further information on restricted variables.

5 Free text comments do not need to be anonymised. A statement has been added to the questionnaire stating that any information provided will be shared with the NHS Trust, CQC and researchers analysing the data. **This does not apply if you are publishing the comments**. Any comments that are published must have any identifiable information removed such as a patients' or staff members' names, ethnicity, condition or health details.

6 The electronic file containing individuals names and addresses should be stored securely (i.e. appropriate controls in place to restrict access to authorised personnel only, and technical and organisational measures in place to prevent unauthorised access, loss, corruption of the data etc.).

Storing completed questionnaires

Completed questionnaires must be stored in a separate location to lists of individual's names and the questionnaires kept until 6 months after the end of fieldwork when they should be destroyed.

All mailing lists of patients' names and addresses should be stored separately to that containing survey data, for example in different password protected folder. Mailing lists of patients' names and addresses must be destroyed when the mailing process is complete.

Further information and questions

For more information please see the Q&A section on the NHS surveys website. If you have any questions please contact the Survey Coordination Centre (team@surveycoordination.com) or CQC (patient.survey@cqc.org.uk).