Confidentiality Advisory Group

Precedent Set Categories

This document contains descriptions of commonly-arising situations which have been identified and discussed at meetings of the CAG, where the expertise of a broad range of members is applied to the establishment of precedent advice.

If an application to CAG falls into one of the categories described below, applicants are able to use the CAG **Precedent Set review pathway** which has been developed to enable a more timely review process for these types of applications.

Guidance on the Precedent Set review pathway and how to submit an application can be found on the HRA website **https://www.hra.nhs.uk/about-us/committees-and-services/confidentiality-advisory-group/cag-precedent-set-review-pathway/**

You should read this before submitting your application, paying particular attention to the relevant Precedent Set category for your application.

The latest version of this document can be found at this location – please check to ensure you are using the latest version.

Review Date: 19 July 2020

Precedent Set categories (click on the link to jump straight to that category)

Category	Description	Submission Advice
1. Participant identification applications (applications to identify a cohort of patients and subsequently seek their consent).	This category can support the recruitment of participants to research studies or surveys, enabling applicants to access data on potential participants in order to send them study invitations or surveys. Section 251 support may be requested to screen patient records to check eligibility, as well as to access patient contact details to send invitation letters. The preferred options for seeking consent are for a member of the care team (who is recognised by the patient as such) to directly ask the service user's permission for the care team to pass on their details to the researcher, or for a member of the care team to pass on information about a study to the service user, who can then contact the researcher if they so wish. This allows the direct care team to determine whether it is appropriate to contact the patient, and engenders the trust of patients, both in the specific activity and in research activity in general. Applications should only be made under this category where the above options are not feasible and the activity can be justified in terms of public interest.	You should explore ways to limit access to patient identifiable data without consent. This could include limiting the length of time the data is accessed, limiting the number of people accessing the data, sending letters on-site to avoid any further processing of identifiable data, and accessing the minimum information necessary in order to identify the cohort. Security assurances must be provided for the site where identifiable service user data will be accessed. The removal of data from the site is to be avoided. Where this process will occur at multiple sites, you may not be required to provide security assurances for each one but will be responsible for ensuring that these are in place and will be complied with. **Exit Strategy** Once consent is obtained, Section 251 support under the Regulations is no longer required. The return of a completed survey or questionnaire may constitute implied consent. Where consent is not obtained the anonymisation/deletion of identifiable data is the appropriate exit strategy.

Category	Description	Submission Advice
2. Access to deceased person's data	This category applies where some or all the entire cohort is deceased. It is clearly not feasible to obtain consent from a person who is deceased. The Next of Kin cannot give consent in this situation, unless they are the Legal Personal Representative or the person administering the estate. In some cases, finding out an individual's mortality status (whether deceased or not) could lead to the further disclosure of identifiable information, and it has been therefore accepted that it is not practicable to do so.	You should consider all practicable alternatives. These could include asking the direct care team to access the data and de-identify it before providing the information, or completing an application to NHS Digital to obtain pseudonymised data on the cohort. If no alternative can be found, the focus should be upon minimising the disclosure of patient confidential information. You should ensure that only information which is necessary for the purpose of the activity is accessed, and for the minimum length of time. Security assurances must be provided for the site where the data is to be accessed. In cases where data will be removed from site for processing, security assurances must be provided for any site where data processing will take place. **Exit Strategy** Anonymisation or pseudonymisation of the confidential patient information is likely to form the exit strategy for an application in this category.

Category	Description	Submission Advice
3. Where applicants are accessing data on-site to extract anonymised data.	The preferred method for access to patient data is for the direct care team to extract and anonymise the information from the case notes, avoiding any breach of patient confidence. Applications under this category should only be made where this method is not practicable and there is justification (in terms of public interest) for the applicant to access patient identifiable data for a short period of time in order to anonymise the data on-site.	You should clearly demonstrate that you have explored all possible practicable alternatives: in addition to asking the direct care team to extract and anonymise the information, applicants could sit in with care teams who provide only the required information from the patient record (limiting researcher access to patient data) or funding care teams to carry out searches. If these options are not practicable, you should explain why not. You must provide security assurances for the site where data is to be accessed, along with confirmation that you and any co-applicant will be compliant with these security arrangements while on-site. Data should not be removed from the site. You should specify the exact length of time for which you require Section 251 support and explain why this time period is necessary. **Exit Strategy** Anonymisation is the required exit strategy for this category. The time taken to extract and anonymise all data is considered on a case by case basis; however an appropriate length of time for data processing under this category would be around 6 months

Category	Description	Submission Advice
4. Time limited access to undertake record linkage/validation and to anonymise the data	This category allows applicants to collect follow-up or additional data on a particular cohort. The data may be added to a dataset that is already held, or the applicant may be asking for a combination of data from two datasets held by a third party (in this case the linkage is carried out by the third party). It may also be used to check that data is correct, for example verifying names and addresses before contacting patients to seek consent for research. Applications under this category most commonly involve NHS Digital (who are the data controller for a number of national datasets), as the third party carrying out data linkage. Such applications typically involve sending identifiers to NHS Digital to obtain data on individuals within a particular cohort. Identifiers will usually include name, NHS number and date of birth to ensure accuracy. NHS Digital extracts the requested data and returns it to the applicant in anonymised form. Section 251 support under this category covers the disclosure of identifiers to the third party for linkage or verification, and also covers the third party to process the data for the specific purpose outlined in the application.	You must already have a legal basis for access to the identifiable data. In some cases, you may be instigating the flow of data without accessing any identifiable data. An example would be where you ask the direct care team, or an organisation holding data on individuals with a particular health condition, to send identifiers to NHS Digital on your behalf so that NHS Digital can return an anonymised dataset to you. Section 251 support is still required to allow the third party to disclose identifiable information on your behalf, and to cover NHS Digital for the data processing. You should liaise with the third party to ensure that you are providing them with the minimum number of identifiers necessary in order to link the datasets. The risk that a patient could be identified from any data returned should be minimal. If the dataset contains identifiers (with the exception of date of death) this will exclude the application from the Precedent Set pathway. The submission of a data flow diagram to illustrate the data flows is particularly important for applications in this category. Information security assurances are not required from NHS Digital, but will be required to cover any other third party processing identifiable data. You should provide security assurances for any site where identifiable data will be processed. Under Regulation 5 of the Control of Patient Information Regulations, favourable REC opinion must be in place for research studies. This will cover the processing (disclosure of identifiers and linkage) even where you are not requesting identifiable data. **Exit Strategy** Anonymisation is the required exit strategy for this category.

Category	Description	Submission Advice
5. Applications utilising the BPSU (British Paediatric Surveillance Unit) methodology or the CAPSS (Children and Adolescent Psychiatry Surveillance System) methodology. **6. Applications utilising the British Opthalmological Surveillance Unit (BOSU) methodology**	The BPSU methodology is used to collect data nationally on rare childhood diseases, to enable research to be carried out where numbers in any one area would be too low due to the rarity of the disease. The BOSU methodology is a surveillance methodology designed to support and enable research for patients with rare eye conditions. Both methodologies use the reporting card system: every month an electronic reporting card with a list of conditions currently under surveillance is sent to consultants and other specialists, who return the card notifying the BPSU/BOSU of any cases they have seen, or stating that they have not seen any cases for this condition. BPSU/BOSU pass the details of clinicians who have reported cases of the relevant condition to the researcher, who will send the clinician a questionnaire for each reported case, requesting pseudonymised, clinical data to be returned for analysis. These methodologies were devised in conjunction with the CAG, to reduce the risk of identifiability where information about small numbers of patients with rare diseases is transferred.	You should illustrate the data flows with a data flow diagram. Although the method of data collection and the data flows should not vary between applications, the data items returned by the clinician to the applicant may differ in each project. You should ensure that the data returned to you from the clinician contains the minimum level of information needed to achieve the aims of the application. In cases where a second questionnaire will be sent to the clinician for follow-up of the patient, it will be necessary to store pseudonymised information in order to link the resulting data – you should ensure that the risk of identifying the individual is minimal. You should not keep identifiers such as date of birth or postcode, unless this can be justified in terms of the study aims. If you are retaining identifiers (except for date of death) the application would be excluded from the Precedent Set pathway. **Exit strategy** Anonymisation of the data is an appropriate exit strategy for this category.

Category	Description	Submission Advice
7. Validity of consent	This applies to situations where the data controller responsible for releasing data states that the wording of the original consent is insufficient to provide a legal basis to for them to allow access to the data. An application under this category should only be made if this decision cannot be resolved locally, and written confirmation from the data controller can be provided. Applications submitted under this category have often been considered by the Independent Group Advising on the Release of Data (IGARD), which approves applications for access to data held by NHS Digital. Where the consent is not clearly applicable to the data requested, IGARD has previously directed applicants to the CAG to ensure a legal basis is in place for access to the data. This category is also used where contact details of participants are held under consent, but need to be validated by requesting up to date details from other sources such as NHS Digital.	You should provide copies of the original patient information leaflets, consent forms and details of any changes to these documents. You should provide evidence of review of consent materials and assessment of validity by the data controller from whom data is being requested. The application cannot be processed without this information. It is important that the information requested should be in the spirit of the original consent provided. Where there is a significant extension from the original consent provided, a new application will need to be made. This will be processed via the most appropriate review pathway. This category cannot be used to significantly extend or vary the terms of the consent, but is intended to resolve issues around the interpretation of the existing consent. **Exit strategy** An appropriate exit strategy for the activity should be described within the application.
8. Data cleansing of historical studies	This typically covers re-collection of data already obtained or new sources of the same data fields to validate current data. If carried out in relation to a pre-existing study, review of previous conditions of support will apply and if there is a significant deviation then this might require full review at a CAG meeting.	You should state whether the application relates to a pre-existing study and outline whether there are any changes to the purpose or methodology of the application, and whether the original conditions of support will be complied with.

Category	Description	Submission Advice
9. Access to mortality, cancer or GP data from NHS Digital ('class support applications')	For activities/studies applying to access mortality, cancer or GP registration data from NHS Digital that have previously accessed data under the NHS Central Register (ECC 2- 04(c)/2010) application. This may also cover historical longitudinal studies that commenced a significant number of years ago that still receive information from NHS Digital, and where NHS Digital has identified that the legal basis to supply the relevant information is no longer clear.	You should evidence that it is not feasible to move towards receiving pseudonymised data from NHS Digital, and that patient objections will be respected
10. Incidental disclosures of identifiable information made to an applicant who is observing practices and procedures within a health and social care setting	This applies to situations where the applicant is likely to be party to identifiable service user data in written or verbal form, although the activity does not concern this data. This may occur during the study of processes in a health setting (analysis of how IT systems are used in a GP surgery) or practices (attending an MDT meeting to study communications between staff groups). Although access to identifiable data is incidental, it still involves a breach of patient confidentiality: the applicant is listening to discussions, or viewing reports, about patients. They will therefore have access to information which would not usually be shared with anyone outside the patients' direct care team.	You should demonstrate that it would be impracticable to seek consent from service users whose data will be disclosed to observers during the course of the activity. There should be no processing of identifiable data and you should consider ways of limiting exposure to identifiable data. The use of audio or written records of identifiable service user information is to be avoided. Security assurances are required for the site where the observations take place. Support will be based on confirmation that the IG Toolkit at the site will be complied with and that no identifiable information will be kept onsite or removed from the site. **Exit strategy** The need for support under the Regulations should be short-lived, as no identifiable data will be retained or removed from site – the analysis will not be concerned with service user information.

Category	Description	Submission Advice
11. Applications made by the Picker Institute Europe to administer surveys on behalf of CQC.	The Picker Institute, Europe, is commissioned by the CQC to administer patient surveys on their behalf. CQC is the data controller for the surveys, bearing overall responsibility for the data processing. Any breaches to the agreed methodology are the responsibility of CQC. Participating NHS Trusts are data controllers in relation to patient data held at hospital sites as part of direct patient care. They have the option to send out the surveys to their patients, however where it is not practicable for staff at the hospital to do this, approved contractors can complete this work on their behalf. Picker Institute applies for Section 251 support on behalf of participating NHS Trusts to cover the provision of patient identifiable information (patient name and address) to contractors, who then send the survey to the patient. Section 251 support also covers the provision of demographic information on all patients who were sent the survey, so that Picker Institute can look at whether the survey responses are representative of the whole population. Approved contractors process the data for the purpose of mailing out surveys to patients. Applications are regularly submitted by the Picker Institute. The methodology remains the same for each survey, although minor changes are regularly made to improve data security and new approaches aimed at improving response rates are frequently piloted.	The methodology for the surveys is approved in principle by the CAG. Any changes to the methodology should be highlighted in the main body of the application and will be considered on a case by case basis by the Sub-Committee. Any changes involving a significant change to data security or data processing, or engaging any of the exclusion criteria listed here, will be referred to a full meeting of the CAG. **Exit Strategy** The support requested is time limited in order to access names and addresses to send out patient surveys. Anonymisation/destruction of identifiable data or consent (implied by the return of a completed questionnaire) form the exit strategy for this category.

Document Control

Change Record

Version Number & Status	Date of Change	Reason for Change
1.1	5 April 2017	First draft of document
1.2	3 July 2017	Second draft of document
1.3	4 July 2017	Third draft of document
1.4	14 July 2017	No change to content – comments on presentation
2.0	19 July 2017	Added numbering, version control and review date

Reviewers

Name (name of reviewer and/or management group reviewing)	Version Reviewed
Confidentiality Advisory Group	1.1
Head of Confidentiality Advice Service/Sue Bourne	1.2
Confidentiality Advice Team	1.3
CAG Management Board	1.4
Head of Confidentiality Advice Service	2.0

Distribution of Approved Versions

Platform (e.g.HRA intranet or website)	Date of Publication	Version Released
HRA website	July 2017	2.0
HRA Hub	19/07/2017	2.0