



Health Research Authority

2 Redman Place
Stratford
London
E20 1JQ

Tel: 020 7104 8100
Email: cag@hra.nhs.uk

14 September 2022

Tamantha Webster
Survey manager
151 Buckingham Palace Road,
London,
SW1W 9SZ

Dear Ms Webster,

Application title: **The 2022 Urgent and Emergency Care Survey**
CAG reference: **22/CAG/0107**

Thank you for your amendment request to the above non-research application, submitted for support under Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002 to process confidential patient information without consent. Supported applications enable the data controller to provide specified information to the applicant for the purposes of the relevant activity, without being in breach of the common law duty of confidentiality, although other relevant legislative provisions will still be applicable.

The role of the Confidentiality Advisory Group (CAG) is to review applications submitted under these Regulations and to provide advice to the Secretary of State for Health and Social Care on whether an application should be supported, and if so, any relevant conditions.

Secretary of State for Health and Social Care support decision

The Secretary of State for Health and Social Care, having considered the advice from the Confidentiality Advice Team (CAT) as set out below, has determined the following:

1. The amendment, to increase the sample size of the cohort from 420 type 3 patients (1370 total), to 580 type 3 patients (1530 total), in Trusts that have type 1 & type 3 departments, is supported, subject to compliance with the standard conditions of support.

Amendment request

This application is to allow the disclosure of confidential patient information from NHS trusts to one of three approved contractors for the purpose of sending out questionnaires for the 2022 Urgent and Emergency Care Survey, and for disclosure of postcode to the Survey Coordination Centre for Existing Methods (SCCEM) at Picker for analysis purposes.

's251' support is currently in place for the following sample sizes;

- Trusts with only Type 1 departments, the sample size is 1250 patients.

- Trusts who have both Type 1 and Type 3 departments will submit a sample size of 950 Type 1 patients and 420 Type 3 patients, a total of 1370 patients.

This amendment sought support for an increase in sample size to the following;

- For trusts with only Type 1 departments, the sample size will remain at 1250 patients.
- Trusts who have both Type 1 and Type 3 departments will submit a sample size of 950 Type 1 patients (no change) and 580 Type 3 patients, a total of 1530 patients.

This is due to a recent decline in responses to the survey.

Confidentiality Advice Team advice

The amendment requested was considered by the Confidentiality Advice Team. No queries were raised regarding this amendment.

Confidentiality Advice Team conclusion

In line with the considerations above, the CAT agreed that the minimum criteria under the Regulations appeared to have been met for this amendment, and therefore advised recommending support to the Secretary of State for Health and Social Care.

Specific conditions of support

1. Confirmation provided from the IG Delivery Team at NHS Digital to the CAG that the relevant Data Security and Protection Toolkit (DSPT) submission(s) has achieved the 'Standards Met' threshold. See section below titled 'security assurance requirements' for further information. **Confirmed:**

The NHS Digital **21/22** DSPT reviews for **Patient Perspective Ltd, Picker Institute Europe and Quality Health Ltd** were confirmed as 'Standards Met' on the NHS Digital DSPT Tracker (checked 12 September 2022)

Reviewed documents

<i>Document</i>	<i>Version</i>	<i>Date</i>
CAG amendment form		17 August 2022
P101769_UEC22_Sampling instructions_V2_CK SG_JKr_20220812_protect	2	12 August 2022

Please do not hesitate to contact me if you have any queries following this letter. I would be grateful if you could quote the above reference number in all future correspondence.

Yours sincerely

Caroline Watchurst
Confidentiality Advisor

On behalf of the Secretary of State for Health and Social Care

Email: cag@hra.nhs.uk

Enclosures: Standard conditions of support

Standard conditions of support

Support to process confidential patient information without consent, given by the Secretary of State for Health and Social Care, is subject to the following standard conditions of support.

The applicant and those processing the information will ensure that:

1. The specified confidential patient information is only used for the purpose(s) set out in the application.
2. Confidentiality is preserved and there are no disclosures of information in aggregate or patient level form that may inferentially identify a person, nor will any attempt be made to identify individuals, households or organisations in the data.
3. Requirements of the Statistics and Registration Services Act 2007 are adhered to regarding publication when relevant, in addition to other national guidance.
4. All staff with access to confidential patient information have contractual obligations of confidentiality, enforceable through disciplinary procedures.
5. All staff with access to confidential patient information have received appropriate ongoing training to ensure they are aware of their responsibilities.
6. Activities remain consistent with the General Data Protection Regulation and Data Protection Act 2018.
7. Audit of data processing by a designated agent is facilitated and supported.
8. The wishes of patients who have withheld or withdrawn their consent are respected.
9. Any significant changes (for example, people, purpose, data flows, data items, security arrangements) must be supported via formal amendment prior to changes coming into effect.
10. An annual review report is submitted to the CAG every 12 months from the date of the final support letter, for the duration of the support.
11. Any breaches of confidentiality around the supported flows of information should be reported to CAG within 10 working days of the incident, along with remedial actions taken / to be taken. This does not remove the need to follow national/legal requirements for reporting relevant security breaches.