National Patient Experience Survey

National Patient Experience Survey Programme

Privacy Impact Assessment (Update 2018)

1. Introduction

The National Patient Experience (NPE) Survey was conducted for the first time in 2017. It is a survey of public, acute, inpatient hospital care and it is the second-largest survey in Ireland, after the national census[1]. 13,706 people participated in the inaugural survey. The NPE Survey is a partnership between the Health Information and Quality Authority (HIQA), the Health Service Executive (HSE) and the Department of Health. The partner organisations have committed to repeating the inpatient survey in 2018 and every year thereafter.

In preparation for the inaugural survey in 2017, the NPE Survey Programme commissioned an independent third party to carry out a Privacy Impact Assessment (PIA).[2] The findings from this PIA informed the development of security and data protection controls for the implementation of the survey. PIAs are, however, conducted at very specific and strategic points in time and as such they cannot capture the natural evolution of the projects they assess. A guidance document published by HIQA in 2017[3] recommends that PIAs should be updated at regular intervals, particularly if projects evolve in a way that introduces new privacy risks. Even if specific processes do not change over a project lifetime, PIAs should be conducted to evaluate the adequacy of security and privacy controls, particularly in light of changes to legislation or, indeed, the introduction of new legislation.

This document presents the privacy risks identified for the survey programme in 2018.

1.1. What is changing in the NPE Survey 2018?

In 2018, a number of changes will affect the implementation of the NPE Survey. In updating the PIA, special consideration was given to the following:

- The General Data Protection Regulation (GDPR) entered into force on 25 May 2018, replacing existing national data protection legislation. As a result, the NPE Survey Programme needed to review its processes, security arrangements and privacy controls to ensure it is compliant with GDPR.
- In 2018, the inclusion criteria changed to include 16 and 17 year olds. This group was not included in the 2017 survey.
- The following changes were made to the 2018 questionnaire: question 55 ('Are you male or female?') was amended and a question on 'reason for admission' was added to the survey. Respondents can choose not to disclose personal information.

[1] https://www.irishtimes.com/news/ireland/irish-news/patient-input-key-to-health-service-provision-says-hiqa-1.3323049

[2] The PIA summary report can be downloaded from: https://www.patientexperience.ie/about-the-survey/information-governance/

[3] Health Information and Quality Authority (2017). Guidance on Privacy Impact Assessment in health and social care. Version 2.0. [online]. Available from: https://www.hiqa.ie/sites/default/files/2017-10/Guidance-on-Privacy-Impact-Assessment-in-health-and-social-care.pdf.

- Following requests from the hospitals, the redaction guidelines for the anonymisation of the free-text questions (Q59-61) were reviewed; ward names and certain professions are no longer anonymised (except in very small hospitals).
- Hospitals can review their performance in the survey, including the qualitative comments, in 'real-time' by accessing a customised reporting facility.

As part of this PIA, the benefits of implementing these changes are evaluated against the potential privacy risks that they pose to the survey programme.

2. Survey model overview

This section provides an overview of the NPE Survey model. This model is closely aligned to that of the national inpatient survey in the United Kingdom.

Step 1: hospitals sample eligible participants during a specific survey month[4] and subsequently share this patient source data with a managed service contracted by HIQA.

Step 2: the managed service records and manages the list of all eligible participants. It removes the names of patients who have opted out of the survey or who may have died since their discharge from hospital. The managed service distributes the survey to all eligible patients via post.

Step 3: eligible patients receive the survey two weeks after their discharge from hospital. They receive two further reminders (including a second survey questionnaire) at two two-week intervals. Eligible participants can complete the survey either online or by filling out the survey and returning it by post. Participants can also choose to opt-out (and in doing so stop further correspondence from the survey programme).

Participants can opt-out of the survey:

- by informing a member of staff when they are being discharged from hospital
- by calling the Freephone number or by sending an email
- on the website www.patientexperience.ie
- by returning a blank survey questionnaire.

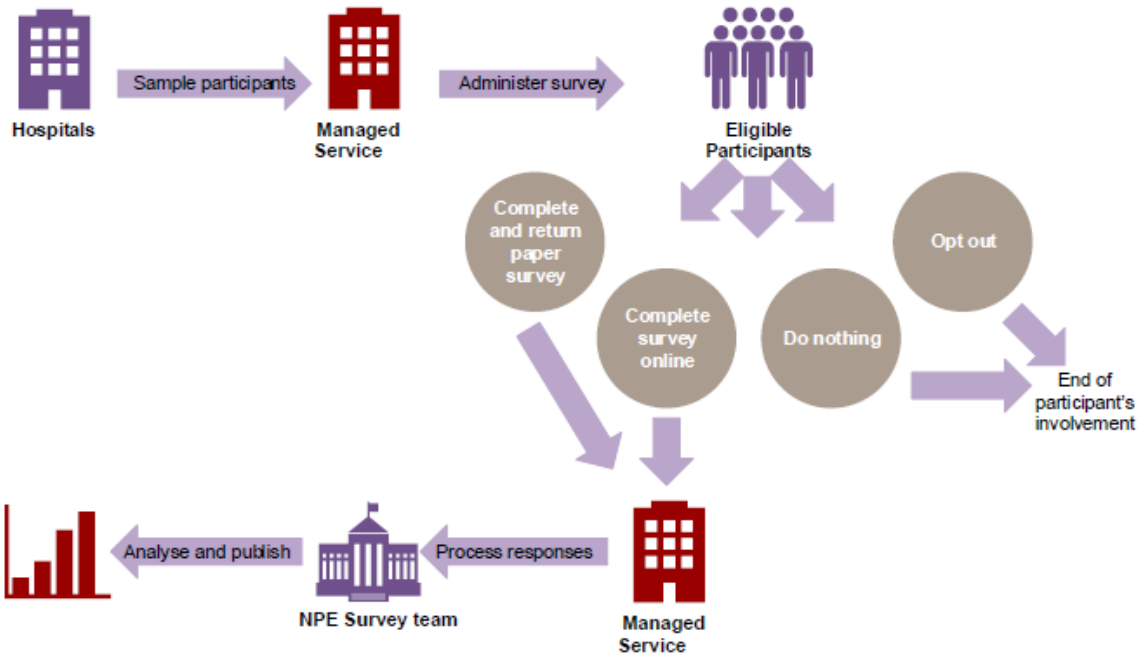
Step 4: all survey responses are returned to the managed service for processing.

Step 5: the processed, cleaned and quality-assured data is sent to the NPE Survey team (based in HIQA) for analysis and reporting.

Figure 1 depicts the NPE Survey model.

[4] In both 2017 and 2018 all eligible participants were inpatients discharged during the month of May.

Figure 1. NPE Survey model



Source: NPE Survey PIA 2017

3. Methodology for the PIA update

The input of stakeholders is an important and recommended step in conducting a PIA. In fact, GDPR emphasises that stakeholders must be involved in the PIA process.[5]

A stakeholder consultation meeting was held in April 2018. This meeting gathered all central stakeholders with substantial knowledge of the NPE Survey project. At the meeting, all existing risks (identified in the 2017 PIA) were reviewed, new risks were identified and a risk register created. The security and privacy controls implemented by the survey programme were also reviewed. Each risk was subsequently assigned a risk rating, ranging from 1 to 25.

Risk ratings were assigned on the basis of the matrix in Figure 2. This matrix combines the impact of a risk with the likelihood of its occurrence. For instance, a risk that is very likely to occur because the controls in place are very strong and which bears only negligible consequences to a data subject's privacy, would be assigned a rating of 5. It was important to achieve consensus during this exercise — final risk ratings were assigned once all participants agreed on a rating. Risks with higher ratings are prioritised during the project implementation phase and are monitored closely by the wider project team.

[5] Health Information and Quality Authority (2017). Guidance on Privacy Impact Assessment in health and social care. Version 2.0. [online]. Available from: https://www.hiqa.ie/sites/default/files/2017-10/Guidance-on-Privacy-Impact-Assessment-in-health-and-social-care.pdf.

Figure 2: Risk matrix structure

	Likelihood				
Impact	Rare 1	Unlikely 2	Possible 3	Likely 4	Highly likely 5
Negligible - 1	1	2	3	4	5
Minor - 2	2	4	6	8	10
Moderate - 3	3	6	9	12	15
Major - 4	4	8	12	16	20
Critical - 5	5	10	15	20	25

Low (1-7) **Medium (8-14)** **High (15-25)**

4. Updated PIA risks

4.1. Inactive risks

One risk was removed from the project risk register as it is no longer an active risk:

Responsibilities are undefined or unclear

Due to the point-in-time nature of this PIA, there is a risk that the responsibilities and boundaries for the roles of data controller and data processor are not clearly defined or assigned to the numerous parties involved (HIQA, HSE, voluntary hospitals, managed service, sub-processors).

During the consultation, the project stakeholders agreed that this risk was no longer valid, and that it was a risk specifically linked to the first year status of the survey in 2017. The stakeholders noted that all project partners were now very clear on their specific roles and responsibilities as either data controllers or data processors. Furthermore, the roles and responsibilities are clearly outlined in the data sharing agreements and business contracts signed by the relevant parties. However, this item is likely to be re-activated as a risk if any of the entities change in the future.

4.2. Project risks, associated controls and risk ratings

#	Privacy risk	Year risk identified	Risk rating
1	**Re-identification using pseudonymised data** There is a risk that administrative data (personal information collected to administer the survey, including patient contact details) is retained until the last pseudonymised survey responses have been processed – approximately two months after the last patients have been sampled. There is a risk that participants' contact details could be linked with their pseudonymised survey responses.	2017	**6** (moderate/ unlikely)
	Proposed management control The risk is controlled through a yearly retention and destruction schedule. This document outlines the reasons for holding on to different categories of data and specifies the timeline for retaining, deleting or destroying data. It should be noted that the risk is valid only until the end of the survey period, that is three months from the survey start or two weeks after the last reminders have been sent out. After this date, participant contact details are permanently deleted and can no longer be linked with survey responses. During the period of risk, administrative data is stored separately from the survey responses. The file containing this administrative data is also password protected. The hardcopy survey responses are held in a locked and secure location. Furthermore, the hardcopy surveys are destroyed at the end of the survey cycle.		

#	Privacy risk	Year risk identified	Risk rating
2	**Participants' self-disclosure of sensitive information** There is a risk that, in answering the three qualitative/open questions, survey participants voluntarily disclose personally identifiable information (PII) or sensitive PII which is not required or sought by the survey. These three questions are: 1. Was there anything particularly good about your hospital care? 2. Was there anything that could be improved? 3. Any other comments or suggestions?	2017	**5** (highly likely/negligible)
	Proposed management control The risk is controlled through the application of strict anonymisation and risk assessment procedures. All qualitative comments are anonymised and risk assessed prior to being uploaded to the database of responses for hospitals to review. The anonymisation procedure removes all personal identifiers relating to a participant or a member of staff. The risk assessment procedure ensures that all anonymised comments are assessed for their compliance with or deviation from quality standards. These comments are logged and used to inform regulation programmes. Qualitative comments are not published in the reporting platform unless 30 or more patients from that particular hospital respond to the survey. In addition, all comments are coded using a framework matrix — this provides hospitals with information on how frequently patients have commented on a specific topic or theme. A selection of anonymised comments is published in national, hospital and hospital group reports.		

#	Privacy risk	Year risk identified	Risk rating
3	**Retention of personal data** There is a risk that participant data (for example, original patient data provided by hospitals or response data) is retained for a period beyond that which is required for the completion of the survey's objectives (that is, from the start of the survey month until the close of the survey 12 weeks later).	2017	**1** (rare/negligible)
	Proposed management control The National Patient Experience Survey does not store participants' contact details beyond the period that is required to administer the survey, and this commitment is outlined in the survey programme's record retention and destruction policy. The risk is therefore fully controlled through the implementation of the survey programme's record retention and destruction policy, including the destruction schedule. These documents explain the rationale for retention and destruction of all data sources containing personally identifiable information (PII). Participant's contact details and other working files containing PII are deleted by the managed service two weeks after the last reminders have been sent out and the last responses have been processed (that is, 12 weeks from the start of the survey). This process is supervised by HIQA. The printing company, contracted by the managed service, responsible for printing and distributing the survey deletes all partial print files (containing only patients' names and addresses) immediately after every mailshot. HIQA will hold on to the anonymous response data indefinitely in order to facilitate secondary as well as trend-analyses over time.		

#	Privacy risk	Year risk identified	Risk rating
4	**Creation of new data hotspots** There is a risk that several new data hotspots are created within different organisations' technical environments during the survey period. Data hotspots may be defined as instances whereby personally identifiable information (PII) or sensitive PII is collected in a way or in a system that is new or that could be vulnerable to an unauthorised disclosure, data breach or security infringement.	2017	**3** (rare/moderate)
	Proposed management control The risk is controlled by the fact that all potential data hotspots have been identified and pre-defined security processes were put in place to minimise the creation of new data hotspots, as well as the management of existing ones. The NPE Survey Programme is bound by the HSE's National I.T. Policies and Standards during the data transfers from hospitals to the managed service. The NPE Survey Programme's security policy and access control policy outline specific provisions which are enforced once the data is transferred and subsequently processed by the managed service. The survey programme also developed a data breach management procedure which will be invoked in the event of a security incident. These policies and procedures remain in force throughout the project life cycle. All data transfers from hospitals to the managed service occur though a secure File Transfer Protocol (sFTP). The transfer of all working files containing PI or PII are encrypted and all data at rest is similarly encrypted.		

#	Privacy risk	Year risk identified	Risk rating
5	**Security controls** There is a risk that the controls, processes and or procedures required by the data controller (HIQA) for managing the security of participants' data are not consistently applied by the managed service (including the primary data processor and its sub-processors).	2017	**8** (unlikely/major)
	Proposed management control The risk is controlled by the survey programme's comprehensive information governance framework, which consists of policies and procedures covering the following areas: data protection and confidentiality, information security, data breach management, record retention and destruction, data access control, business continuity, and record management. All persons working on or on behalf of HIQA and the managed service receive training on these policies and are required to adhere to all provisions outlined therein. Specifically, project staff must report data breaches and follow breach notification and management procedures.		

#	Privacy risk	Year risk identified	Risk rating
6	**Unauthorised disclosure of participants' recent hospital visit** There is a risk that surveys issued to participants (via the post) may be accessed by unauthorised individuals, disclosing the fact that the intended recipient was recently discharged from hospital after receiving medical treatment.	2017	**1** (rare/negligible)
	Proposed management control The risk has been addressed by packaging the surveys and reminder letters in unbranded white envelopes. As the packaging does not contain the logo of the NPE Survey Programme it would be difficult for anyone to deduce the sender, unless of course, the letter was opened.		

#	Privacy risk	Year risk identified	Risk rating
7	**Processor transparency** There is a risk that, despite significant efforts (including a national media campaign, information leaflets, information sessions with hospital staff, information packs handed to patients upon discharge and a dedicated website), survey participants may not be fully aware of who will process or have access to their data or survey responses.	2017	**12** (possible/major)
	Proposed management control This risk has been addressed by numerous efforts undertaken to explain the survey programme's information-handling practices. A patient information leaflet and invitation letter are handed to patients upon discharge. This material provides participants with information to consider their participation in the survey. In addition, a dedicated page on information governance has been created on www.patientexperience.ie. On this site, a statement of purpose, statement of information practices, data protection and confidentiality policies are available for download. These documents provide a comprehensive oversight of the information-handling practices of the National Patient Experience Survey Programme. The patient information leaflet has been amended in 2018 to include a notice on the potential further processing of (anonymous) survey responses by health service researchers under agreed conditions. In addition, a national media campaign informs the public about the NPE Survey Programme. Any documents produced by the programme adhere to NALA guidelines.		

#	Privacy risk	Year risk identified	Risk rating
8	**Right to object to processing** There is a risk that the survey opt-out process does not adequately facilitate the patient to object to the processing of their personal data (i.e. to opt out) upon their initial engagement with the survey when being discharged from hospital. Additionally, participants may not be fully aware of, or consent to, their personal data being uploaded from hospitals to the managed service for the purposes of the survey.	2017	**1** (rare/negligible)
	Proposed management control The National Patient Experience Survey is being conducted in the public interest. Participation is entirely voluntary, therefore participants are not under any obligation to respond to the survey. Respondents also control what information they provide in the survey questionnaire. The risk has been addressed by the survey programme's facilitation of opt-out requests from patients while they are still in hospital. A process has been developed to allow patients to opt out of the survey during the discharge process. Should a patient wish to opt out, a member of staff notes the patient's name and date of birth on the back of the information pack handed to the patient upon discharge, and sends this to a nominated individual within the hospital. The person's name will subsequently be removed from the list of patients eligible to take the survey. Furthermore, the survey programme allows participants to opt-out using four additional methods (listed on page 3 of this document).		

#	Privacy risk	Year risk identified	Risk rating
9	**Right to obtain personal data** There is a risk that, during the survey period, an adequate process may not be in place to facilitate individuals to obtain their personal data via a subject access request (SAR).	2017	**1** (rare/negligible)
	Proposed management control The risk has been addressed through the development of a subject access request policy and associated procedure. The NPE Survey Programme's subject access request policy allows individuals (data subjects) to request access to a copy of their personal data stored by the programme. In order to retrieve information held on a data subject, access requests must be received prior to the deletion of patients' contact details as personal information cannot be recovered once the administrative data has been deleted. The access request policy and associated procedure have been updated to include the shorter processing timelines required under GDPR. The data subject access request policy is available to download from www.patientexperience.ie. Further information on processing timelines can also be found on the survey programme's website.		

#	Privacy risk	Year risk identified	Risk rating
10	**Self-disclosure of sensitive personal information in response to two new questions** In 2018, a question was added to the survey asking respondents to specify their reason for admission to hospital. Question 55 ('Are you male or female?') was also amended and now includes a third response option. There is a risk that, in the event of a data breach, self-disclosed sensitive information may be used in conjunction with other information to identify an individual, thereby compromising their privacy. In the context of GDPR, medical information is considered sensitive personal information.	2018	**4** (rare/major)
	Proposed management control The risk is mitigated by the IT security controls and processes deployed throughout the project life cycle. The risk is limited to the survey period — which is two weeks after the last reminders have been sent out or twelve weeks from the start of the survey. Once patients' contact details have been deleted, the risk is no longer valid. It is worth highlighting that survey participants are free to skip any questions they do not wish to answer.		

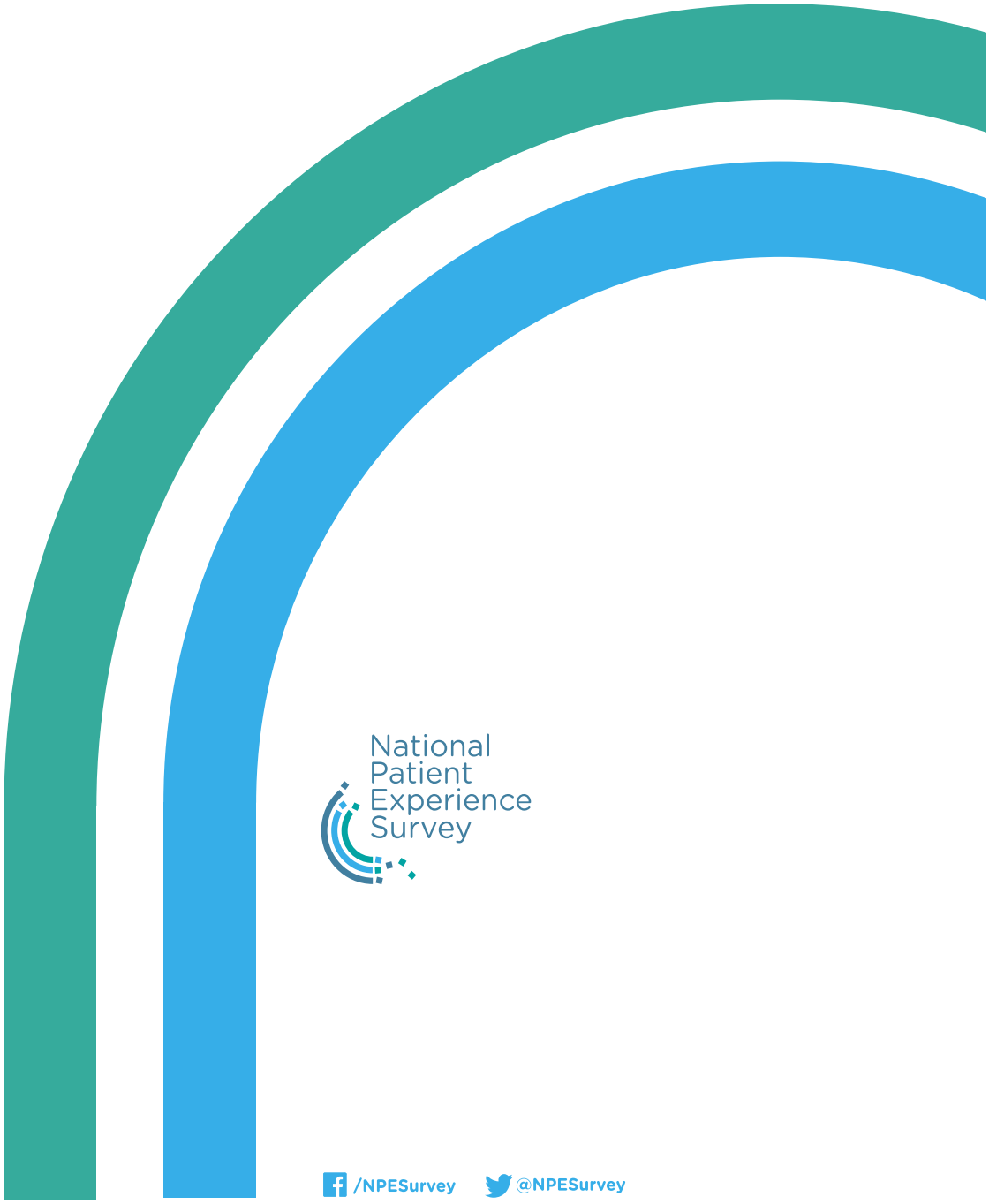
#	Privacy risk	Year risk identified	Risk rating
11	**Changes to anonymisation criteria** Hospital staff have access to the qualitative survey responses for their hospital via a reporting platform. In 2018, the anonymisation guidelines for the redaction of qualitative comments were amended — ward names and specific healthcare professions (for example, physiotherapists, speech and occupational therapists) are no longer anonymised. The decision to 'relax' anonymisation criteria was made following feedback from hospital staff who said that they often could not action patient suggestions for improvement due to a lack of important contextual details. There is a risk that hospital personnel will be able to identify specific patients or hospital staff on the basis of responses to Q59-61. This risk is disproportionately higher in smaller hospitals who employ fewer staff and who have less than 30 discharges per month.	2018	**2** (unlikely/ negligible)
	Proposed management control In this instance, the benefits of changing the redaction guidelines outweigh the risks of identifying individual participants or members of hospital staff. It should be noted that the risk is unlikely to exist in bigger hospitals. Furthermore, it should be noted that a maximum of three individuals in each participating hospital have access to the reporting platform. Given that individuals with access to the platform tend not to be frontline staff, the risk of identification is further minimised. The NPE Survey team in HIQA verify the correct application of anonymisation criteria for all patient comments prior to their release on the reporting platform for hospitals. Comments for smaller hospitals are reviewed on a case-by-case basis, acknowledging the ease of identification in smaller hospitals. The risk is thus controlled.		

#	Privacy risk	Year risk identified	Risk rating
12	**Personal information solicited by helpdesk operators** There is a risk that Freephone helpline operators may unnecessarily request personal details or information when dealing with queries from a member of the public.	2018	**3** (possible/ negligible)
	Proposed management control The risk has been significantly reduced by the fact that the helpline scripts have been purposefully amended to ensure that operators do not request personal information from a caller unless they are required to complete a specific action for which personal information is absolutely necessary. Unless callers seek to explicitly opt-out of the survey, ask for a new questionnaire/Freepost envelope or opt-out on behalf of a deceased relative (who had been eligible to participate in the survey), helpline operators do not request personally identifiable information. Operators may ask callers for their survey code, but only if they need to verify the 'participant status' of a caller.		

#	Privacy risk	Year risk identified	Risk rating
13	**Secondary processing** There is a risk that participants are unclear about the fact that their survey responses may be used for secondary research purposes (including, for example, publication in scientific journals, presentations at conferences).	2018	**2** (unlikely/ negligible)
	Proposed management control The risk is controlled by making patients aware of the potential secondary analysis of survey responses. In the interest of transparency, the participant/patient information leaflet has been amended to include a notice on secondary processing of survey responses. Secondary analysis is carried out on fully anonymised data.		

#	Privacy risk	Year risk identified	Risk rating
14	**Non-processing of in-hospital opt-outs** There is a risk that even though a mechanism is in place to facilitate patients to opt out of the survey while they are still in hospital (and before their data is processed), hospital staff receiving the request may not relay the request to the nominated individual within the hospital. There is a possibility that patients may receive a survey pack in the post despite their explicit objection to the processing of their contact details.	2018	**12** (possible/major)
	Proposed management control The NPE Survey Programme relies on 'public interest' to carry out its annual survey of inpatient experience. Nonetheless, the programme respects the rights of individuals to object to the processing of their contact details for inclusion in the survey sample, and therefore implements a process to facilitate patients to opt-out of the survey while they are still in hospital. It is a distinct possibility that amidst their day-to-day workload, hospital staff may forget to process patient opt-out requests. In an effort to mitigate this risk, the in-hospital opt-out process has been documented in the NPE Survey processes guide and distributed to participating hospitals in advance of the survey month. Furthermore, during their hospital roadshow, members of the NPE team covered the in-hospital opt-out process in their presentations to hospital staff. It should also be noted that when the NPE Survey team engaged with hospital personnel on this issue, they found that the frequency of in-hospital opt-out requests was very small.		

#	Privacy risk	Year risk identified	Risk rating
15	**Data breach during data extraction** There is a risk that during the data extraction phase (the survey month plus one week) patients who do not meet the eligibility criteria are wrongfully included in the survey sample. For example, day-case, outpatient, maternity or psychiatric patients could erroneously be included in the sample. There is a further risk that ineligible patients may receive, complete and return a survey questionnaire.	2018	**12** (possible/major)
	Proposed management control The risk is controlled through a quality assurance (QA) process which takes place at two different levels. Once the data is extracted, a nominated individual within each hospital quality-assures the extract and specifically checks for the correct application of the survey eligibility criteria before renaming the data file to indicate its QA status. In addition, a nominated person within the HSE quality assures every hospital extract before it is processed by the managed service. This process is intended to keep data breaches to an absolute minimum. Breaches that occur within the data extraction process are dealt with by the data protection officers within each participating hospital. Furthermore a system has been developed by the managed service to suppress ineligible survey responses.		


National
Patient
Experience
Survey
/NPESurvey
@NPESurvey