National Patient Experience Survey

National Patient Experience Survey

Privacy Impact Assessment 2019 (Update)

1. Introduction

The National Patient Experience Survey is a nationwide survey asking people for feedback about their stay in hospital. The survey is a partnership between the Health Information and Quality Authority (HIQA), the Health Service Executive (HSE) and the Department of Health. All patients aged 16 and over discharged each May, who spend 24 hours or more in a public acute hospital and have a postal address in the Republic of Ireland are asked to complete the survey.

In preparation for the inaugural survey in 2017, the National Patient Experience Survey Programme commissioned an independent third party to carry out a Privacy Impact Assessment (PIA).[1] The findings of this PIA informed the development of security and data protection controls for the implementation of the first 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.

Guidance on Privacy Impact Assessment in health and social care published by HIQA in 2017[2], 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 at regular intervals to evaluate the adequacy of security and privacy controls, particularly in light of changes to current legislation or the introduction of new legislation.

This report presents the findings from a stakeholder consultation to update the PIA for the 2019 iteration of the National Patient Experience Survey.

2. Why are we updating the PIA?

In preparing for the survey in 2019, special consideration was given to the following:

- the General Data Protection Regulation (GDPR) (EU) 2016/679 and the Data Protection Act 2018 place additional responsibility and accountability on data controllers as well as data processors. Specifically, the GDPR and the Data Protection Act 2018 oblige data controllers to carry out and continually update a PIA if they process personal and or sensitive information.
- it is important to review and evaluate the adequacy of security controls in mitigating the privacy risks identified in the 2017 and 2018 PIAs.

[1] The 2017 and 2018 PIA can be downloaded from: https://www.patientexperience.ie/about-the-survey/information-governance/.
[2] 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.

3. Survey model

3.1. Overview of the National Patient Experience Survey model

This section provides an overview of the National Patient Experience Survey model.

Step 1: hospital staff provide patients with a letter and a Frequently Asked Questions (FAQ) flyer upon discharge, which inform them that they may be invited to participate in a survey. Patients can opt out of the survey at this stage.

Step 2: each of the 40 participating hospitals identify eligible participants' contact data during the month of May and subsequently share this patient source data with Behaviour and Attitudes, the data processor.

Step 3: the data processor records and manages the list of all eligible participants for the 40 participating hospitals. It removes the names of patients who have opted out of the survey or have died since their discharge from hospital. The data processor distributes the survey to all eligible patients via post.

Step 4: eligible patients receive the survey approximately two weeks after their discharge from hospital. They receive two further reminders (including a second survey) at two two-week intervals. Eligible participants respond to the survey either online or by completing the paper version and returning it by post.

Participants can opt out of the survey:

- while they are still in hospital
- by calling the Freephone number
- by email
- on the website www.patientexperience.ie
- by returning a blank survey questionnaire.

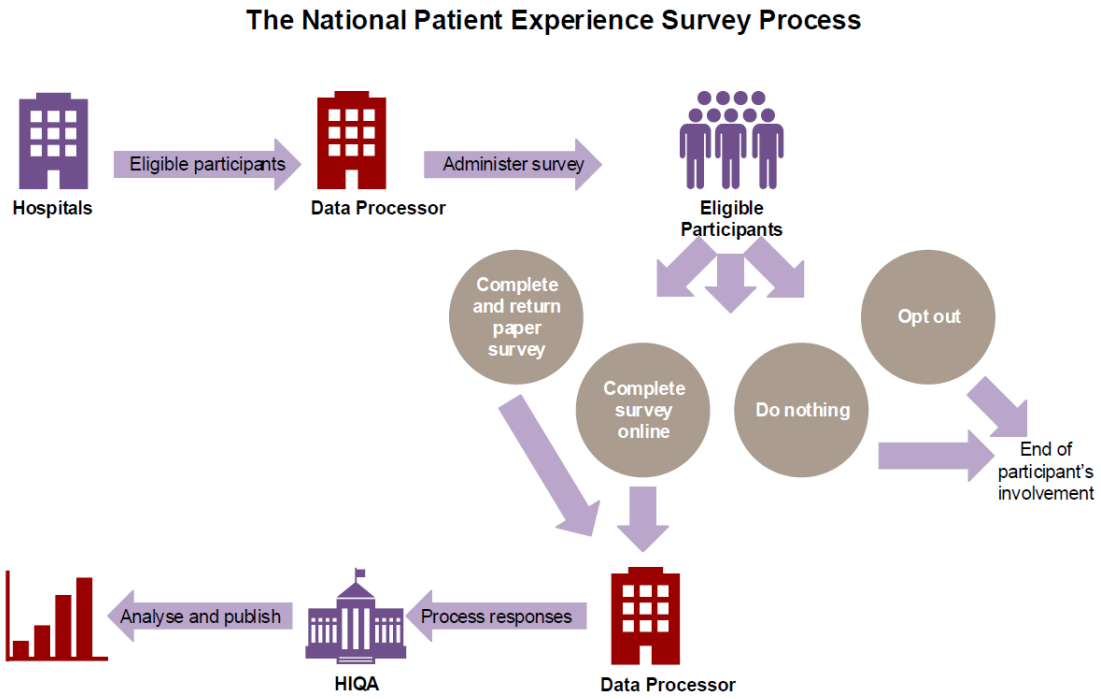
Step 5: all hard copy survey responses are returned to the data processor for processing.

Step 6: the processed, cleaned and quality assured data is sent to the National Patient Experience Survey team for analysis and reporting.

Step 7: the contact details of the eligible participants and hard-copy survey responses are destroyed in line with a retention and destruction schedule. For more information on the schedule and the survey's information governance, please see www.patientexperience.ie.

Figure 1 depicts the National Patient Experience Survey model.

Figure 1: National Patient Experience Survey model



4. Methodology to update the 2019 PIA

4.1 Risk assessment process

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

A stakeholder consultation meeting was held in April 2019. This meeting involved all central stakeholders with substantial knowledge of the National Patient Experience Survey project. At the meeting, all existing risks (identified in the 2018 PIA) were reviewed and the risk register was updated. Security and privacy controls were also reviewed. Risks were 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.

Figure 2: Risk Matrix

	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)**

5. Data privacy risk register

5.1. Identification of new project risks

No additional risks were identified during the consultation with stakeholders.

5.2. Risks that are no longer valid

Risk numbers 9 and 10, outlined below, were removed from the 2018 project risk register.

Privacy Impact Assessment 2018, risk number 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 data subject access request.

It was agreed during the stakeholder consultation to remove risk number 9: 'right to obtain personal data', as a Subject Access Request policy and procedure has been developed and is compliant with data protection legislation. The Data Subject Access Request policy and form are available on www.patientexperience.ie.

Privacy Impact Assessment 2018, risk number 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.

During the consultation, the project stakeholders agreed that this risk is no longer valid as no sensitive information was disclosed in 2018 in spite of the inclusion of two new questions. In addition, risk number 2, 'participants' self-disclosure of sensitive information', outlines the proposed management controls for the disclosure of any sensitive data.

5.3. Updated risk register

#	Privacy risk	Year risk identified	Change to control (Yes/No)	Risk rating
1.	**Re-identification using pseudonymised data** 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 six weeks after the last patients have been sampled. There is a risk that participants' contact details could be linked with their pseudonymised survey responses.	2017	**No**	**6** (Unlikely/ moderate)
	Proposed management control The risk is controlled through a yearly retention and destruction policy and schedule, which outline 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, four months from the beginning of the survey or six weeks after the closure of the survey. 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	Change to control (Yes/No)	Risk rating
2.	**Participants' self-disclosure of sensitive information** There is a risk that, in answering the three qualitative/open-ended 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? In addition, participants may indirectly identify themselves through their answers to any of the 58 quantitative questions, for example by indicating their reason for admission in question 54.	2017	**No**	**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 an online reporting tool, where nominated hospital staff can view survey responses. The anonymisation procedure removes personal identifiers relating to a participant or a member of staff. Qualitative comments submitted online are reviewed and redacted by the National Patient Experience Survey team in HIQA, whereas the paper responses are transcribed and anonymised by researchers in the data processor. All comments are reviewed individually by the National Patient Experience Survey team to ensure the anonymisation criteria have been applied correctly and consistently. Comments are then risk assessed internally in HIQA prior to being released onto the response database.			

	The risk-assessment procedure ensures that all anonymised comments are assessed for their compliance with or deviation from quality standards. This procedure assigns a risk rating to every comment describing a deviation from a standard. Comments are subsequently assessed in terms of the severity of impact and likelihood of recurrence. Comments are then logged and used to inform regulation programmes. Hospital staff are not given access to the qualitative comments in the online reporting tool 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. This analysis will form the basis of reporting of the qualitative comments in aggregate form for the national, hospital group and hospital level reports. A selection of anonymised comments is also published in the reports.

#	Privacy risk	Year risk identified	Change to control (Yes/No)	Risk rating
3.	**Retention of personal data** There is a risk that participant data (for example, original patient data provided by the hospitals, or the survey response data) is retained for a period beyond that which is required for the completion of the survey's objectives.	2017	**No**	**8** (unlikely/ major)
	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 Record Retention and Destruction policy.			

	The risk is therefore fully controlled through the implementation of the Record Retention and Destruction policy, including the retention and destruction schedule. These documents explain the rationale for the retention and destruction of all data sources containing personally identifiable information (PII). Participants' contact details and other working files containing PII are deleted by the data processor within six weeks of the closure of the survey and the last responses have been processed (that is, four months from the start of the survey). The hardcopy responses are held for an additional two months from the end of the survey to ensure that there are no issues with the processed responses and will subsequently be destroyed. In both instances the destruction of data is supervised by HIQA. Print files and other partial files containing personal information, generated to administer the survey and manage the sample, will be deleted once they have served their purpose. Print files will be erased immediately after each print cycle by a file-eraser programme, which will be overseen by the data processor's IT Manager. All other partial files created will be destroyed immediately after they have served their purpose, or at the latest at the end of the National Patient Experience Survey cycle. The eight character unique survey codes assigned to individual participants are destroyed within two months of the closure of the survey cycle. All original, soft-copy survey response files will be destroyed following the anonymisation and risk rating of the data, and the creation of a final, redacted survey-response file. Destruction of the original unanonymised survey-response file will be conducted within two months of the closure of the survey and aligned to related data-destruction processes, to ensure consistency. All survey response files will be audited, to ensure that the remaining controlled copy of each annual survey is the final anonymised version. Once the destruction schedule has been executed, it will no longer be possible to link individuals to their survey responses. HIQA will retain the anonymous response data indefinitely in order to facilitate secondary as well as trend analyses over time.

#	Privacy risk	Year risk identified	Change to control (Yes/No)	Risk rating
4.	**Creation of new data hotspots** There is a risk that several new data hotspots are created within different organisation's technical environments during the survey period. Data hotspots may be defined as instances where 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	**Yes**	**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 National Patient Experience Survey is bound by the HSE's national IT policies and standards during the data transfers from hospitals to the data processor. The National Patient Experience Survey is underpinned by a comprehensive information governance framework consisting of policies, procedures and processes. A security policy and access control policy outline specific provisions which are enforced once the data is transferred and subsequently processed by the data processor. The survey programme also developed a data breach management procedure which will be invoked in the event of a security incident. The policies and procedures remain in force throughout the project life cycle.			

	Data processing agreements have been signed between HIQA and the data processor. These agreements formally authorise the sharing and processing of data required for the implementation of the National Patient Experience Survey. The data processor has achieved, and is re-certified annually, to the international information-security standard ISO27001:2013. Appropriate contractual arrangements and obligations are in place with the data processor to ensure that the National Patient Experience Survey management team has the ability to perform security reviews or audits of security aspects of third-party processing activities, by a data processor and or data sub-processor. All data transfers from hospitals to the data processor 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	Change to control (Yes/No)	Risk rating
5.	**Security controls** There is a risk that the controls, processes, procedures and training required by the data controller (HIQA) for managing the security of participants' data are not consistently applied within the data processor and or its sub-processors.	2017	**No**	**8** (unlikely/ major)
	Proposed management control The information governance framework outlines the various security controls implemented in the course of the National Patient Experience Survey. In particular, a security policy, data breach management procedure and record retention and destruction policy and schedule outline the various principles and provisions underpinning the implementation of the survey. Furthermore, process specifications for the security and management of participants' personal data have been specified, agreed and documented.			

	The programme's Access Control Policy specifies user-access rights in the data processor and describes the controls implemented to limit access to personal data on the basis of business requirements. The responsibility for data breach management in the context of the National Patient Experience Survey rests with the Data Protection Officer in HIQA, who assists the National Patient Experience Survey in complying with data protection legislation, including GDPR and the Data Protection Act 2018. Appropriate contractual arrangements and obligations have been agreed with the data processor to ensure that the National Patient Experience Survey management team has the ability to perform security reviews or audits of security on all data-processing activities. Within the programme's information governance documentation, the process specifications for the extraction and processing of patient source data and survey responses are outlined and specified. These pertain to information security, user access management, and encryption protocols for the sharing of personal information, security incident and data breach management. All potentially personal information is audited prior to processing. This includes the original data extracts containing eligible participants' contact information and the anonymised survey responses, which are used for primary analysis by HIQA and for secondary analysis by academic and other institutions, upon agreement. All persons working for or on behalf of HIQA and the data processor receive training on these policies and are required to adhere to all provisions outlined therein. Specifically, staff working for or on behalf of the National Patient Experience Survey must report data breaches and follow breach notification and management procedures.

#	Privacy risk	Year risk identified	Change to control (Yes/No)	Risk rating
6.	**Unauthorised disclosure of participants' recent hospital visit** There is a risk that surveys issued to participants (via post) may be accessed by unauthorised individuals, disclosing the fact that the intended recipient was recently discharged from hospital after receiving medical treatment.	2017	**No**	**1** (rare/ negligible)

	Management response/control The risk that unauthorised individuals may access or intercept the survey pack or reminder letters sent by the National Patient Experience Survey is a risk inherent to any survey or communication of a private and sensitive nature (for example, bank statements). The outer packaging of the National Patient Experience Survey pack is discrete, serving to deflect interest of third-party individuals. The survey pack is enclosed in a white, non-branded envelope. As a result of the discrete packaging it is not evident that the intended recipient was recently discharged from a hospital.

#	Privacy risk	Year risk identified	Change to control (Yes/No)	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 at 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	**Yes**	**6** (possible/ minor)
	Proposed management control This risk has been addressed by numerous efforts undertaken to explain the survey's information-handling practices. A patient information leaflet and invitation letter are handed to patients upon discharge to inform them that they will be invited to participate in the National Patient Experience Survey. The patient information leaflet was 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 dedicated page on information governance was created on www.patientexperience.ie. On this site, a statement of purpose, a statement of information practices, and a data protection and confidentiality policy are available for download. These documents provide comprehensive oversight of the information-handling practices for the National Patient Experience Survey. In addition, a national media campaign informs the public about the National Patient Experience Survey. Any documents produced for the National Patient Experience Survey adhere to National Adult Literacy Agency (NALA) guidelines.

#	Privacy risk	Year risk identified	Change to control (Yes/No)	Risk rating
8.	**Right to object to processing** There is a risk that the survey opt-out process does not adequately facilitate the patient in objecting to their personal data being processed (that is, opting out) 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 data processor for the purposes of the survey**.**	2017	**No**	**1** (rare/ negligible)
	Proposed management control The National Patient Experience Survey is being conducted in the public interest. The patient-source data gathered by hospitals and processed by the data processor is the minimum information necessary to implement a national survey of inpatient experience. Participation in the survey 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 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. The information pack, which contains the name and date of birth of the patient who wishes to opt out, is securely destroyed. Furthermore, eligible participants can opt out using four additional methods (listed on page 3 of this document). Individuals who opt out of the National Patient Experience Survey, upon or following discharge, will be removed from the contact list and will not receive any further communication in relation to the survey.

#	Privacy risk	Year risk identified	Change to control (Yes/No)	Risk rating
9.	**Changes to anonymisation criteria** Hospital staff have access to the qualitative survey responses for their hospital via the online reporting tool. 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 questions 59, 60 and 61. This risk is disproportionately higher in smaller hospitals who employ fewer staff and who have less than 30 discharges per month.	2018	**NA** (new control)	**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. Since the introduction of the online reporting tool in 2017, hospitals can only gain access to the qualitative data on the online reporting tool once they have received a minimum of 30 responses to the survey. Furthermore, it should be noted that a maximum of three individuals in each participating hospital have access to the online reporting tool. Given that individuals with access to the tool tend not to be frontline staff, the risk of identification is further minimised. The National Patient Experience Survey team verify the correct application of anonymisation criteria for all patient comments prior to their release on the online reporting tool for hospitals. Comments on 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	Change to control (Yes/No)	Risk rating
10.	**Personal information solicited by helpdesk of the Freephone number** 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	**NA** (new control)	**3** (possible/ negligible)
	Proposed management control The risk has been significantly reduced by the fact that helpline scripts have been purposefully developed 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.			

	A record is created for every call the helpline receives. Access to these records is restricted and only four people within the data processor, where helpline staff are based during the survey period, can access the records. Participants who opt out of the survey are logged in the master file. The helpline records are deleted and shredded at the end of the survey period.

#	Privacy risk	Year risk identified	Change to control (Yes/No)	Risk rating
11.	**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, presentation at conferences).	2018	**NA** (new control)	**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 FAQ (Frequently Asked Questions) distributed to patients upon discharge, and the information letter which accompanies the first distribution of the survey two weeks after discharge, were amended in 2018 to include a notice on secondary processing of survey responses. Secondary analysis is carried out on fully-anonymised data. Only anonymised, qualitative comments are published in reports and secondary publications. The risk is justified on the basis of ethical imperatives — the primary reason for collecting patient experience data is to provide service providers, planners and policy makers with information on patients' experiences that they can incorporate into the planning and design of improved service delivery. As such, the survey is conducted in the public interest. The survey data is a very rich source of information and there is a lot of scope for secondary analysis. Disseminating survey research in peer-reviewed journals and at conferences is a very important and effective forum for dissemination.			

#	Privacy risk	Year risk identified	Change to control (Yes/No)	Risk rating
12.	**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	**NA** (new control)	**9** (possible/ moderate)
	Proposed management control The National Patient Experience Survey relies on 'public interest' to carry out its annual survey of inpatient experience. Nonetheless, the survey 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 National Patient Experience Survey Process Guide. The process guide details the data-extraction and opt-out processes and is distributed to participating hospitals in advance of the survey month. It should also be noted that when the National Patient Experience 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	Change to control (Yes/No)	Risk rating
13.	**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	**NA** (new control)	**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 data processor. 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 in each participating hospital. Furthermore, a system has been developed by the data processor to suppress ineligible survey responses.			

6. Next steps

This document reflects the feedback from all stakeholders in relation to identified risks for the National Patient Experience Survey 2019 and will be published on www.patientexperience.ie.

National Patient Experience Survey