NATIONAL PATIENT EXPERIENCE SURVEY PROGRAMME PRIVACY IMPACT ASSESSMENT (PIA) - SUMMARY REPORT

INTRODUCTION

This Privacy Impact Assessment ("PIA") summary report was prepared for the Health Information and Quality Authority ("HIQA") for the sole purpose of assessing the privacy impact on the National Patient Experience Survey ("NPE Survey") participants.

The PIA was conducted by Mazars, a professional services firm that specialises in providing independent privacy consultancy services including the review of practices for handling personal data.

Mazars reviewed the processes associated with the collection, management and security of participant-related data including administrative data, which includes personal and personally identifiable information such as patients' contact details as well as the survey responses.

Upon conclusion of the PIA, the National Patient Experience Survey Programme undertook to address identified risks via tailored remediation plans.

HIQA is registered as a Data Controller with the Office of the Data Protection Commissioner ("DPC") (reference number: 9768/A).

BACKGROUND

The National Patient Experience Survey is a partnership between the Health Information and Quality Authority (HIQA), the Health Service Executive (HSE) and the Department of Health and is the first of its kind in Ireland. It gives patients an opportunity to describe their experiences during their recent stay in hospital and this information will be used to improve the Irish health service. HIQA, as the lead partner in this initiative, is responsible for the implementation of the National Patient Experience Survey.

The National Patient Experience Survey Programme is the first of its kind in Ireland. It gives patients an opportunity to describe their experiences during their recent stay in hospital and this information will be used to improve the Irish health service.

HIQA has contracted a third party, Behaviour & Attitudes to administer the National Patient Experience Survey.

All adult patients, who have spent more than 24 hours in a public acute hospital and are discharged during the month of May 2017 will be invited to participate in the National Patient Experience Survey. Patients will be asked 61 questions on topics related to various aspects of the care they received in hospital.

Participants will receive a survey pack in the post two weeks after they have been discharged. They will also receive two reminder letters provided they have not yet returned a survey. Eligible participants can choose to opt-out of the survey while still in hospital or after being discharged.

The results of the survey will be published in December 2017. The national, hospital group and hospital reports will be available to download from www.patientexperience.ie.

Figure 1 below outlines the high-level process of the National Patient Experience Survey.

The National Patient Experience Survey Process

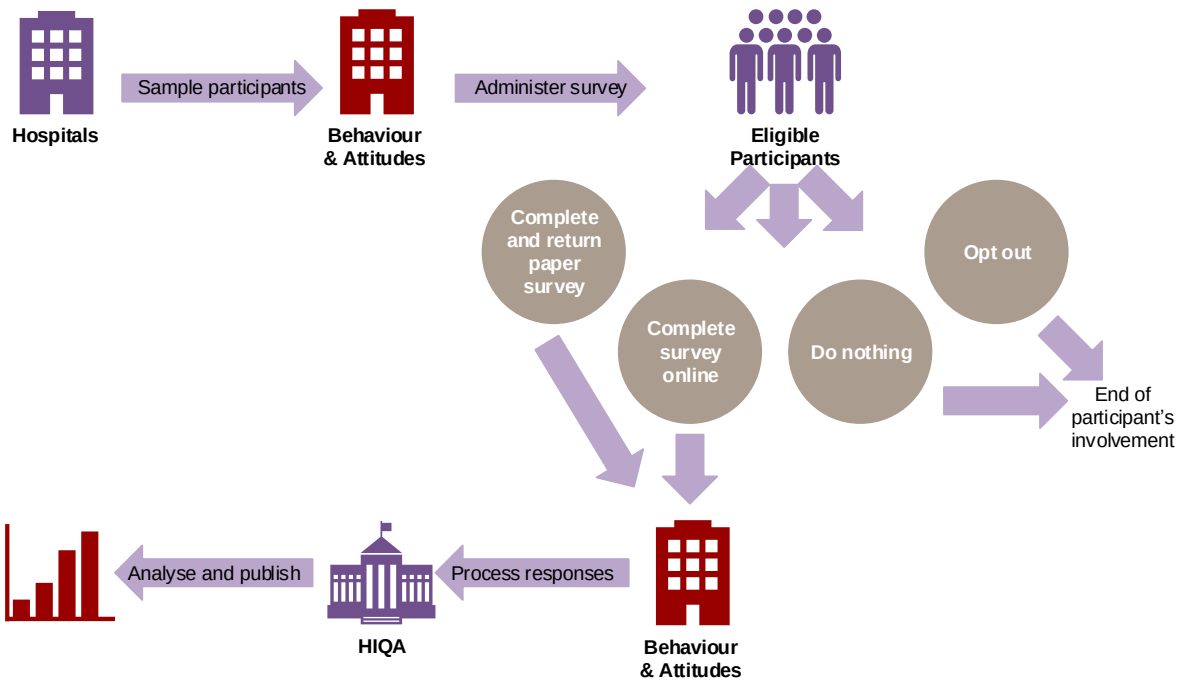

Figure 1: The National Patient Experience Survey process

HIQA acts in the capacity of the data controller for all of the data that it or Behaviour & Attitudes collects as part the National Patient Experience Survey.

Behaviour & Attitudes acts in the capacity of data processor on behalf of HIQA for all of the data that it collects as part of the National Patient Experience Survey.

THIS DOCUMENT

The above introduction and background sections were prepared by HIQA. The remaining sections of this report have been prepared by Mazars for the purpose of providing a summary of the PIA. This summary does not disclose all details on the risks identified or remediation actions taken.

Mazars assumes no responsibility in respect of, or arising out of, or in connection with the contents of this document to parties other than to the NPE Survey programme. If others choose to rely in any way on the contents of this report they do so entirely at their own risk.

WHAT IS A PRIVACY IMPACT ASSESSMENT?

A Privacy Impact Assessment (PIA) is a process of systematically considering the potential impact a project or proposed change will have on the privacy of individuals. By completing a PIA, it is possible to not only identify potential privacy issues at the outset of a project but also to design more effective processes for processing personal data and introduce efficient privacy enhancing operations upon completion of the project.

The Mazars PIA methodology uses a standard set of 11 privacy principles. These principles are consistent with the Organisation for Economic Co-operation and Development (OECD), European

Union (EU) and national legislation, including the Irish Data Protection Act and the General Data Protection regulation (GDPR), and reflect available best practice guidelines.

WHY IS A PIA IMPORTANT?

A PIA helps organisations identify the risks or potential risks to individuals' privacy that may result from new projects, the introduction of new technology, processes or processing activities. It assists in the evaluation of potential solutions to those risks and sets out recommendations design privacy into the proposed solutions.

WHAT DID THE PIA CONCLUDE?

The PIA identified ten privacy risks within the early phase of project design. These risks were reported to HIQA and the NPE Survey Programme steering group for consideration.

WHAT DID HIQA DO ABOUT THESE PRIVACY RISKS?

HIQA and the NPE Survey Steering Group considered the recommendations of the PIA. Remediation actions to address each of the risks identified (see table below) were agreed by the NPE Survey Steering Group.

#	Privacy Risk	Agreed Management Actions (NPE Survey Programme)
1.	**Re-identification Using Pseudonymised Data** Administrative data (personal information collected to administer the survey, including patient contact details) are 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.	The risk has been addressed through the development of a retention and destruction schedule, which outlines the reasons for holding on to different categories of data and specifies for how long data is kept and when it is deleted or destroyed. The risk is valid only until the end of the survey cycle, which is two weeks after the last reminders have been sent out. After this date all participant contact details are permanently deleted and can no longer be linked with survey responses. During the time period that the risk is valid, administrative data is stored on a separate server from the survey responses. The hardcopy survey responses are held in a locked and secure location.
2.	**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).	The risk has been addressed by a series of Data Sharing Agreements that have been signed by HIQA and the Chief Executives and General Managers of all participating hospitals. These agreements formally authorise the sharing of personal information for the purpose of administering the survey. A contract and a data sharing agreement have been put in place between HIQA and Behaviour & Attitudes. These documents define the arrangements for the secure sharing, storage, handling and processing of all data collected during National Patient Experience Survey.
3.	**Participants' Self-Disclosure of Sensitive Information** There is a risk that Survey participants voluntarily disclose personally identifiable	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. The

#	Privacy Risk	Agreed Management Actions (NPE Survey Programme)
	information (PII) or sensitive PII, which is not required or sought by the survey, in answering the three qualitative or open questions. 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?	anonymisation procedure will remove any personal identifiers relating to a participant or a member of staff. The risk assessment procedure will ensure that all anonymised comments are assessed for their compliance with or deviation from quality standards, logged and inform regulation programmes. All comments are thematically coded. This analysis will form the basis of reporting of the qualitative comments in aggregate for the national, hospital group and hospital level reports.
4.	**Retention of Personal Data** There is a risk that participant data (e.g.: original patient data provided by the hospitals, or the response data) is retained for a period beyond that which required for the completion of the survey's objectives (i.e.: May – July 2017).	The risk has been addressed by the Programme's record retention and destruction schedule which explains the rationale for retention and destruction of all data sources containing personal information (including PII). All administrative data including participant contact details is deleted two weeks after the last reminders have been sent out and the last responses have been processed. Behaviour & Attitudes will destroy all administrative data and this process will be supervised by HIQA. The National Patient Experience Survey does not store personal data beyond the period that is required to administer the survey, and this commitment is outlined in the Programme's record retention and destruction policy. HIQA will hold onto the anonymous response data for longer than seven years to facilitate secondary as well as trend analyses over time.
5.	**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.	The risk is controlled by the fact that all potential data hotspots have been identified and pre-defined security processes 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 I.T. Policies and Standards during the data transfers from hospitals to Behaviour & Attitudes. The National Patient Experience Survey Programme's security policy and access control policy outline specific provisions which are enforced once the data is transferred and subsequently processed by Behaviour & Attitudes. The 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.
6.	**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 within the third parties that make up the Managed Service's environment (the primary Data Processor is Behaviour & Attitudes and its sub processors).	The risk is controlled by the 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 Behaviour & Attitudes have received training on these policies and are required to adhere to all provisions outlined therein.

#	Privacy Risk	Agreed Management Actions (NPE Survey Programme)
7.	**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.	The risk has been addressed through use of packaging for the surveys and reminder letters that have no logos. The National Patient Experience Survey packs (containing an invitation letter, a survey questionnaire and a Freepost envelope) and reminder letters are sent to participants in non-branded white envelopes. Therefore, it is not evident that intended recipients were recently discharged from hospital.
8.	**Processor Transparency** There is a risk that, despite significant efforts (including a national media campaign, information leaflets, information sessions with hospital staff, patient information packs 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.	This risk has been addressed by various efforts undertaken to explain the programme's information handling practices. A patient information leaflet and invitation letter will be handed to patients upon discharge. This material provides participants with necessary 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 policy are available for download. These documents provide a comprehensive oversight on the information handling practices of the National Patient Experience Survey.
9.	**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 (i.e. opting out) at their initial engagement with the Survey, i.e. during discharge within the 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**.**	The risk has been addressed by the Programme's facilitation of opt-out requests from patients while still in hospital. A process has been developed that allows patients to opt out of the survey during the discharge process when they receive the survey information pack. A member of staff notes a patient's name and date of birth on the back of the information pack and sends this to the Patient Administration System (PAS) office. The person's name will subsequently be removed from the list of patients eligible to take the survey.
10.	**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 own personal data via a subject access request (SAR).	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. All access requests must be received prior to the deletion of administrative data. 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 Programme's website.