



**Health
Information
and Quality
Authority**

An tÚdarás Um Fhaisnéis
agus Cáilíocht Sláinte

Health Information
and Standards

Summary Report: Data Protection Impact
Assessment (DPIA) for the National Engagement
on Digital Health and Social Care

June 2023

Safer Better Care

About the Health Information and Quality Authority (HIQA)

The Health Information and Quality Authority (HIQA) is an independent statutory authority established to promote safety and quality in the provision of health and social care services for the benefit of the health and welfare of the public.

HIQA's mandate to date extends across a wide range of public, private, and voluntary sector services. Reporting to the Minister for Health and engaging with the Minister for Children, Equality, Disability, Integration, and Youth, HIQA has responsibility for the following:

- **Setting standards for health and social care services** — Developing person-centred standards and guidance, based on evidence and international best practice, for health and social care services in Ireland.
- **Regulating social care services** — The Chief Inspector within HIQA is responsible for registering and inspecting residential services for older people and people with a disability, and children's special care units.
- **Regulating health services** — Regulating medical exposure to ionising radiation.
- **Monitoring services** — Monitoring the safety and quality of health services and children's social services, and investigating as necessary serious concerns about the health and welfare of people who use these services.
- **Health technology assessment** — Evaluating the clinical and cost-effectiveness of health programmes, policies, medicines, medical equipment, diagnostic and surgical techniques, health promotion and protection activities, and providing advice to enable the best use of resources and the best outcomes for people who use our health service.
- **Health information** — Advising on the efficient and secure collection and sharing of health information, setting standards, evaluating information resources and publishing information on the delivery and performance of Ireland's health and social care services.
- **National Care Experience Programme** — Carrying out national service-user experience surveys across a range of health services, in conjunction with the Department of Health and the Health Service Executive (HSE).

Background to the National Engagement on Digital Health and Social Care

The National Engagement on Digital Health and Social Care aims to understand the opinions and attitudes of both the Irish public and professionals working in health and social care in relation to the digitalisation of health and social care services. The engagement is being conducted in the context of EU targets where the public will have electronic access to their medical records by 2030.⁽¹⁾ In addition, under the Sláintecare health reform programme, the Government has goals around using digital technologies in health and social care.⁽²⁾ Furthermore, the engagement is being carried out in light of potential changes to service delivery brought about by the COVID-19 pandemic and changes in attitudes to eHealth information technologies following the cyber-attack in the HSE. It is important to seek the public's and professionals' views on these changes.

This new engagement through surveys and focus groups will gather hard evidence on opinions, attitudes, and comfort levels around accessing and sharing health and social care information digitally as well as digital care. It will look at what these mean to the Irish public and professionals in health and social care, people's expectations, how they would like to use digital information and technology, and where people are in terms of their readiness for such information and services. What professionals and the public see as gaps, challenges, and benefits will also be examined.

HIQA's previous National Public Engagement on Health Information aimed to understand the opinions and attitudes of the Irish public in relation to the collection, use, and sharing of personal health information.⁽³⁾ The key objective was to listen to the voice of the public, understand the findings, and make measurable improvements to how personal health information is collected, used, and shared in Ireland.⁽³⁾

The National Engagement on Digital Health and Social Care builds on the health information engagement by aiming to understand the opinions and attitudes of both the Irish public and professionals in relation to the digitalisation of health and social care services.

The findings will help in the development of national policies around digital health and social care information and services as well as appropriate regulations and legislation. The findings can help bring the public and professionals on board and progress the aims of the Government's eHealth and digital health targets under Europe's Digital Decade: Digital Targets for 2030.⁽¹⁾ In addition, the findings will be used to help deliver fundamental

elements of Sláintecare,⁽²⁾ especially in relation to patient data and information and in implementing technology and eHealth solutions.

This engagement is part of a people-led digitalisation process in line with Sláintecare, Europe's Digital Decade, and the WHO's Global Strategy on Digital Health 2020-2025.^(1,2,4) The partnership approach and engagement also underlie HIQA's mission of protecting service users and working with stakeholders to enhance and enable equity, quality, and safety of health and social care services for all people in Ireland.

The findings of the National Engagement on Digital Health and Social Care will be made available on www.hiqa.ie.

Table of Contents

1. Purpose of this Document..... 6

2. Why is it important to do a DPIA? 6

3. What is the legal basis for processing data?..... 6

4. Roles and Responsibilities 7

5. Lifecycle of the National Engagement Survey Data 7

6. Methodology to Conduct the DPIA..... 9

7. Overview of Risk 11

 7.1 Risks and Controls..... 11

8. Next Steps..... 16

9. References 17

1. Purpose of this Document

This document summarises the findings of a Data Protection Impact Assessment (DPIA). The DPIA was carried out to identify and mitigate risks that survey and focus group participants who will be invited to take part in the National Engagement on Digital Health and Social Care may encounter.

2. Why is it important to do a DPIA?

When personal, sensitive, and special-category data is processed, a DPIA must be carried out to identify and mitigate risks to the privacy of data subjects.

To carry out the National Engagement on Digital Health and Social Care, HIQA will process the data of survey and focus group participants. There will be two surveys, one with the public and one with professionals in health and social care.

The target sample for the public telephone survey is 1,920 people, aged 18 and over. A further 40 to 80 members of the public will participate in focus groups.

The target sample for the online survey is 672 professionals in health and social care. These professionals will come from dentistry, medicine, midwifery, nursing and pharmacy, pre-hospital emergency care, psychology, or will be registered with CORU (Ireland's multi-profession health regulator). A further 40 to 80 professionals across health and social care will participate in focus groups.

A DPIA is necessary to ensure that all risks to the privacy of survey and focus group participants are identified and appropriate safeguards are put in place.

3. What is the legal basis for processing data?

The National Engagement on Digital Health and Social Care complies with data protection laws, including the General Data Protection Regulation (GDPR) 2018.

As per Article 6 (1)(e) of the GDPR and Section 38 Data Protection Act (2018), survey and focus group participants will be explicitly asked to provide their informed consent for the processing of their information.

As per Article 9 (2)(i) of the GDPR and Section 53 Data Protection Act 2018, processing is necessary for reasons of public interest in the area of public

health, as set out in law and subject to suitable and specific measures being in place.

The National Engagement on Digital Health and Social Care also aligns with HIQA's remit under Section 8(1)(i) and Article 8 (1)(j) of the Health Act 2007. This is to provide advice and make recommendations to the Minister for Health about deficiencies identified in information gathered on health services and the general health and welfare of the population.

4. Roles and Responsibilities

HIQA is the data controller for data processed as part of the National Engagement on Digital Health and Social Care. HIQA has contracted an external data processor, IPSOS MRBI, which is responsible for the administration of the public survey. Further information is provided in section 5, Lifecycle of the National Engagement on Digital Health and Social Care Survey Data. IPSOS MRBI, in its role as a managed service, is also responsible for the recruitment of certain members of the public to focus groups. These are people who are identified as having positive, negative, or neutral attitudes to digital health and social care. Further information on this is also available in section 5.

5. Lifecycle of the National Engagement Survey Data

This section provides an overview of the lifecycle of the data collected to conduct the National Engagement on Digital Health and Social Care survey for the public and professionals in health and social care.

Stage one: To source participants for the public survey, telephone numbers will be generated at random and tested to ensure that they are live. Following that, an interviewer will call the number and apply the eligibility criteria by ensuring that the potential survey participant who has answered the call is 18 years of age or over.

The survey for professionals in health and social care will be promoted by HIQA in conjunction with the HSE among professionals to ensure the required numbers complete the survey. A stakeholder engagement plan has been developed for this work.

Both the public and professional surveys will:

- provide information on the aims of the survey
- ask the potential survey participant if they would like to participate and if they consent to their data being processed.

Stage two: Public survey participants will be asked to provide information about themselves, such as their age and level of education, and provide feedback on a number of questions including information access and sharing, sharing health information online, and digital care.

Professional survey participants will be asked demographic questions such as their role, age (by categorisation), the sector they work in, and be presented with questions in relation to digital health and social care.

Stage three: The public survey participant responses will be securely uploaded and stored in a participant response file on the data processor's systems. Participants' responses will be stored separately to survey participants contact details.

The health and social care professional survey will be conducted on HIQA's survey platform. The professionals' survey will be fully anonymous from the start. No questions will be asked that could be used to identify respondents.

Stage four: All focus groups will be conducted by HIQA. Focus groups will take place with members of the public, patient representatives, and representatives of special interest groups. Focus groups will also be carried out with different categories of professionals in health and social care, for example, nurses, general practitioners, or pharmacists. In addition, HIQA will carry out focus groups with administrator and managerial staff as well as information and communications technology (ICT) staff in health and social care to gather their views.

Focus groups will be recorded using MS Teams. Only anonymised data will be retained in the transcriptions and no individual will be identifiable from the information. The focus groups will take place after the survey responses have been collected and analysed because the survey responses will inform the questions in the focus groups. Potential focus group participants will be:

- provided with information on the aims of the national engagement
- given information on how the focus groups will be conducted
- asked if they would like to participate and if they consent to their data being processed.

Stage five: The findings of focus groups will then be combined with the findings of both survey responses. The findings will be analysed and a report published.

Stage six: A data retention and a destruction schedule will be implemented.

The contact details of the public survey participants will be destroyed within four weeks of the survey closing. The data processor will securely transfer the anonymised participants' responses from the survey to HIQA and will delete same from their servers by 28 August 2023.

The survey for professionals in health and social care will be stored on HIQA's survey platform. Once the survey has closed, responses will be downloaded by the HIQA project team to a folder on the HIQA server that is limited to that team only. The data will then be fully deleted from HIQA's survey platform.

The contact details of focus group participants will be destroyed immediately after the focus group meetings.

The anonymised responses of both the public survey and the professionals' survey will be retained by HIQA indefinitely.

The audio recordings of the focus groups will be deleted from HIQA systems in line with the document retention and destruction schedule after the recordings have been transcribed. No personal identifiable information on the focus group members will be transcribed.

6. Methodology to Conduct the DPIA

The DPIA was conducted as per the steps outlined in the [Privacy Impact Assessment toolkit for health and social care](#),⁽⁵⁾ developed by HIQA. The steps were as follows:

Step one: A threshold assessment was conducted. A threshold assessment is a short, initial assessment of a project to determine if a DPIA is required. GDPR states that a DPIA is required when any personal data is processed. Conducting the National Engagement on Digital Health and Social Care involves processing personal information. For the public survey, first name, telephone number, questions on demographic information such as age and gender, along with health status questions will be collected. The professional online survey does not request name or telephone numbers but will collect information such as age category. Therefore, a DPIA is required.

Step two: A data map is developed. The data map outlines the journey the data takes from its point of collection through to its use, distribution, and destruction. It is used to identify potential risks to personal information throughout the data's lifecycle. Key stakeholders, such as the project team who will process the data and the National Engagement on Digital Health and Social Care Steering Group, were consulted and involved in identifying risks.

The DPIA must also determine if the data processing is necessary and proportionate. This means that data should only be collected if the data has a specific use and if there is no other and less intrusive way to collect and process the data. For example, questions used in both surveys and focus groups are assessed to ensure that they are both relevant and that the answers will be used to make measurable improvements in the public's and professionals' wants, needs, and readiness for digital health and social care, including potential impacts for both groups.

Step three: With the input of stakeholders, controls were identified and put in place to reduce the risks as identified in step two. For example, to reduce the risk that individuals may disclose unsolicited, sensitive, health information to HIQA via digitalsurvey@hiqa.ie (as outlined in risk number three in section 7.1 of this document), the following three controls were identified:

- HIQA does not request personal data from members of the public or professionals who contact them
- HIQA receives emails on secure, encrypted, password-protected devices
- HIQA deletes all emails at the end of the engagement project.

A risk rating from 1 to 25 is then assigned to each risk to determine its severity. 1 is the lowest rating and 25 is the highest, as per Table 1 in section 7. For example, the risk that consent is not explained adequately to participants and that they are not provided with the correct information to make an informed decision about participating in the survey (as outlined in risk number four in section 7.1 of this document) represents a low risk and therefore receives a risk rating of 4.

Step four: The DPIA report was produced. The report was reviewed by senior management and approved by the Director of Health Information and Standards. The report was submitted to and subsequently approved by HIQA's Data Protection Officer (DPO). The Technical Standards team in the Health Information and Standards directorate will implement the national engagement.

Step five: The findings of the DPIA are incorporated into the project plan to ensure that all controls are put in place. For example, the timelines for data destruction are incorporated into the project plan.

7. Overview of Risk

The DPIA identified five risks, which are summarised below. The safeguards put in place to mitigate the risks are also summarised in this section. Each risk is assigned a risk rating on the basis of the matrix in Table 1 below. This matrix combines the likelihood of harm to a data subject, based on a scale of 1 to 5, with the severity of harm caused to the data subject, also based on a scale of 1 to 5. For instance, a risk that is almost certain to occur but only bears negligible consequences to a data subject’s privacy would be assigned a rating of 5.

Table 1: Risk Matrix

	Impact→				
Likelihood ↓	Negligible 1	Minor 2	Moderate 3	Significant 4	Substantial 5
Almost certain 5	5	10	15	20	25
Likely 4	4	8	12	16	20
Possible 3	3	6	9	12	15
Unlikely 2	2	4	6	8	10
Rare 1	1	2	3	4	5

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

7.1 Risks and Controls

This section provides an overview of five risks identified in the DPIA and the controls put in place to mitigate each risk.

Risk 1: Data breach

There is a risk that during the collection, retention, transfer, and or destruction of data, personally identifiable and or sensitive data could be lost or disclosed in error. This would represent a data security breach.

Controls

The following controls will be put in place:

HIQA

- adheres to HIQA’s Data Protection and Information Governance policies and standard operating procedures (SOPs)
- provides information governance training for staff responsible for collecting, handling, and analysing data
- applies a data retention and destruction schedule to ensure that data is only retained for the minimum amount of time necessary
- follows a data breach management procedure, which staff are trained on
- only approves the transfer of data using Athena software, which is approved by HIQA
- conducts any online meetings via MS Teams, which is HIQA approved
- will destroy focus group recordings in line with the document retention and destruction policy
- has oversight of contracts with any sub-processors used by the data processor
- ensures the data processor adheres to data de-linking and data destruction processes as agreed.

Managed Service:

- complies with the requirements of the professional code of conduct applicable to all registered market research companies (ICC/ESOMAR International Code on Market, Opinion and Social Research and Data Analytics)
- adheres to the managed service’s IT Security and Information Management policies
- conducts digital meetings via MS Teams, which will be arranged by HIQA
- adheres to the existing contract agreed with HIQA and the defined statement of works for the engagement project, processing all data securely as outlined in that document.

Risk-rating: 6 (unlikely/moderate) – this represents a **low** risk.

Risk 2: Non-adherence to processes and procedures

There is a risk that data processing activities are not conducted in line with agreed policies and procedures, for example, the data is not destroyed in line with the retention and destruction schedule.

Controls

HIQA:

- adheres to the existing contract already in place with the managed service. The associated statement of works for the engagement defines the data-processing activities necessary carry out the project
- adheres to HIQA's policies and procedures and where necessary, develops project specific policies and or procedures, for example data is destroyed in line with the Health Information and Standards - Record Retention Schedule and the specific Record Retention Schedule for the engagement
- provides training on information governance to all staff involved in processing data
- holds routine meetings with the managed service to ensure that all actions are completed as agreed
- oversees a timeline of actions or project plan for the managed service
- has oversight of contracts with any sub-processors used by the managed service
- has developed and oversees the implementation of a retention and destruction schedule
- stores focus groups participants' contact information separately to the findings of focus groups
- stores all project information on HIQA's internal information management platform, SharePoint.

Managed Service:

- adheres to stipulations as per the existing contract between HIQA and the Managed Service and the associated statement of works for this project
- uses Athena data-sharing software to transfer data securely between itself and HIQA
- destroys all data it holds in adherence with the data retention and destruction schedule
- provides an update on all data processing actions completed at routine project meetings
- stores contact details of survey participants separately to their responses.

Risk-rating: 6 (possible/minor) – this represents a **low** risk.

Risk 3: Receipt of sensitive health information via digitalsurvey@hiqa.ie

There is a risk that individuals may disclose unsolicited sensitive information about their healthcare to HIQA via digitalsurvey@hiqa.ie or any other email address used by the project.

Controls

HIQA:

- does not request personal data from members of the public or professionals who contact it
- ensures the digitalsurvey email is only accessible to three named staff from the Technical Standards Team
- follows the Receipt of Unnecessary Personally Identifiable Information – Standard Operating Procedure.

Risk-rating: 6 (unlikely/moderate) – this represents a **low** risk.

Risk 4: Transparency and consent

There is a risk that consent is not explained adequately to participants and they are not provided with the correct information to make an informed decision to participate.

Controls

HIQA:

- ensures the project is conducted in line with ethics approval from the Royal College of Physicians of Ireland
- ensures the project is properly governed through a Steering Group
- approves a telephone script for IPSOS MRBI to use when inviting participants to take the survey over the telephone
- provides focus group and survey participants with information about how their data will be processed if they choose to participate
- asks for the consent of focus group participants and facilitates opt-outs where necessary
- ensures that all communications for public dissemination are accessible and adhere to HIQA plain English guidelines
- ensures all documentation for the public and professionals is reviewed by the HIQA Communications Team
- provides an online FAQ and Participant Information Leaflet, outlining details of the project, including its data-processing activities and information governance on www.hiqa.ie
- ensures all FAQs and Participant Information Leaflets are translated to Irish and are available on the HIQA website
- ensures all FAQs and Participant Information Leaflets are also available in paper format if necessary
- adheres to HIQA's Data Subject Access Request and procedure policy.

Managed Service:

- applies the telephone script approved by HIQA when inviting participants to take the survey
- provides public survey participants with information about how their data will be processed if they choose to participate
- asks for and records consent of public survey participants
- facilitates opt-outs where necessary
- puts in place a process to send public survey participants an FAQ and Participant Information Leaflet by post, if requested.

Risk rating: 4 (unlikely/minor) – this represents a **low** risk.

Risk 5: Receipt and recording of personal and or sensitive information

There is a risk that those conducting the focus groups and telephone surveys will accidentally record or transcribe personal information that is not required or sought by the survey or focus groups.

Controls

HIQA:

- develops and approves all scripts for focus groups and the public survey, therefore avoiding soliciting personal, sensitive, and or extraneous information
- develops anonymisation criteria for the survey responses in the event that participants disclose personal and or sensitive information which is not solicited by the surveys
- ensures all survey responses, audio recordings, and transcripts of audio recordings are saved in a restricted folder
- ensures audio recordings of focus groups are deleted from HIQA systems in line with the document retention and destruction schedule after the recordings have been transcribed.

Managed Service:

- adheres to stipulations as per the existing contract between HIQA and the Managed Service and the associated statement of works
- stores contact details of survey participants separately to their responses
- follows the telephone script as developed by HIQA, therefore avoiding the receipt of personal or sensitive information

- anonymises all personal and or sensitive information disclosed by survey participants at the point of collection.

Risk-rating: 2 (rare/minor) - this represents a **low** risk.

8. Next Steps

This document reflects the feedback from all stakeholders in relation to identified risks for the National Engagement on Digital Health and Social Care Survey and will be published on www.hiqa.ie.

9. References

1. European Commission Europe's Digital Decade: Digital Targets for 2030. Available from: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en. Accessed on: 12 October 2022.

2. Committee on the Future of Healthcare. Committee on the Future of Healthcare Sláintecare Report. Available from: <https://assets.gov.ie/22609/e68786c13e1b4d7daca89b495c506bb8.pdf>. Accessed on: 24 August 2021.

3. HIQA. Health Information Quality Authority. Findings of the National Public Engagement on Health Information, 2021. Available from: <https://www.hiqa.ie/reports-and-publications/health-information/national-public-engagement-health-information>. Accessed on: 08 April 2022.

4. World Health Organization. Global strategy on digital health 2020-2025. 2020. Available from: <https://www.who.int/docs/default-source/documents/g4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf>. Accessed on: 26 August 2021.

5. HIQA. Health Information Quality Authority. Guidance on Privacy Impact Assessment in health and social care 2017. Available from: <https://www.hiqa.ie/sites/default/files/2017-10/Guidance-on-Privacy-Impact-Assessment-in-health-and-social-care.pdf>. Accessed on: 08 April 2022.



Published by the Health Information and Quality Authority (HIQA).

For further information please contact:

Health Information and Quality Authority

George's Court

George's Lane

Smithfield

Dublin 7

D07 E98Y

+353 (0)1 814 7400

info@hiqa.ie | www.hiqa.ie

© Health Information and Quality Authority 2023