



DRAFT

DATA SHARING AGREEMENT

Between

[Department of Social Protection] |

and

[Health Information and Quality Authority]

Pursuant to

The Data Sharing and Governance Act 2019

For the purpose of

[Facilitating the National End of Life Survey.]



Table of Contents

Interpretation Table	3
1. Evaluation for a Data Protection Impact Assessment (DPIA).....	5
2. Purpose of the Data Sharing	7
3. Data to be shared	10
4. Function of the Parties.....	12
5. Legal Basis.....	13
6. Impetus for Data Sharing.....	16
7. Categories of Data Shared	17
8. Duration and Frequency	18
9. How data will be processed.....	19
10. Restrictions.....	22
11. Security Measures	23
12. Retention	32
13. Methods Used to Destroy/Delete Data.....	33
14. Withdrawal from Agreement.....	34
15. Other Matters.....	35
16. Schedule A - Data Protection Impact Assessment.....	37
17. Schedule B	46
18. Schedule C	50
19. Authorised Signatory	51



Interpretation Table

DEFINITION	MEANING
Data controller	Has the meaning given to it by the General Data Protection Regulation (2016/679).
Party disclosing data	Shall mean the Party transferring personal data to the receiving Party or Parties.
Party receiving data	Shall mean the Party receiving personal data from the Party disclosing data.
Data Protection Impact Assessment(DPIA)	Means an assessment carried out for the purposes of Article 35 of the General Data Protection Regulation.
GDPR	Shall be taken as a reference to the General Data Protection Regulation (2016/679) including such related legislation as may be enacted by the Houses of the Oireachtas.
Lead Agency	Refers to the Party to this agreement who is responsible for carrying out the functions set out in 18(2), 18(3), 21(3), 21(5), 22(1), 55(3), 56(1), 56(2), 57(4), 58, 60(1) and 60(4) of the Data Sharing and Governance Act 2019.
Personal Data	Has the meaning given to it by the General Data Protection Regulation (2016/679).
Personal data breach	Has the meaning given to it by the General Data Protection Regulation (2016/679).
Processing	Has the meaning given to it by the General Data Protection Regulation (2016/679).
Public Service Body (PSB)	Means a Public Body as defined by section 10 of the Data Sharing and Governance Act 2019.
Shared personal data	Means data shared pursuant to this agreement.

Table 1.0



Data Sharing Agreement

BETWEEN

Insert name of Lead Agency, having its registered address at:

LEAD AGENCY NAME	ADDRESS
Department (Dept.) of Social Protection	Arás Mhic Dhiarmada, Store Street, Dublin 1

AND

Insert name(s) of Other Party/Parties to the agreement, having its registered address at:

PARTY NAME	ADDRESS
Health Information and Quality Authority (HIQA)	Unit 1301, City Gate, Mahon, Cork T12 Y2XT, Ireland

The Parties hereby agree that the **Dept. of Social Protection** will take the role of Lead Agency for the purpose of this Data Sharing Agreement.

Each of the Parties to this agreement are data controllers in their own right when processing personal data on their own behalf, for their own purposes.



1. Evaluation for a Data Protection Impact Assessment (DPIA)

The completion of a DPIA can help data controllers to meet their obligations in relation to data protection law. [Article 35](#) of the GDPR sets out when a DPIA is required.

Data controllers should periodically re-evaluate the risk associated with existing processing activities to understand if a DPIA is now required.

1.1 Identifying if a DPIA is required

The below checklist can assist organisations to understand if they require a DPIA pursuant to Article 35 GDPR to support their data sharing agreement. The questions should be answered in relation to the entire project that the data share corresponds to. This ensures that Public Service Bodies (PSBs) have the opportunity to be transparent in the evaluation of risks in relation to the data required for this process.

The completion of a DPIA is relevant to this data sharing agreement as you will be asked to provide a summary of any DPIA carried out in [Section 16](#) of this document.

The questions below should be completed by the Lead Agency together with the Other Parties involved in this data sharing agreement. Please contact your DPO in relation to the requirement to carry out a DPIA.

	DOES THE PROCESS INVOLVE:	YES/NO
1.1.1	Processing being carried out prior to 25th May 2018?	[NO]

Table 1.1

If 'Yes' proceed to [1.2](#)
If 'No' proceed to [1.1.2](#)

	DOES THE PROCESS INVOLVE:	YES/NO
1.1.2	A new purpose for which personal data is processed?	[NO]
1.1.3	The introduction of new types of technology?	[NO]

Table 1.2

If 'Yes' to either of the last two questions, proceed to [1.1.4](#).
If 'No' to both of the last two questions, proceed to [1.2](#).

	DOES THE PROCESS INVOLVE:	YES/NO
1.1.4	Processing that is likely to result in a high risk to the rights and freedoms of natural persons?	[Choose Y/N]

Table 1.3

If 'Yes', then you are likely required to carry out a DPIA under [Article 35](#) GDPR.
If 'No' proceed to [1.2](#).



1.2 Further Considerations

There are limited circumstances where a mandatory DPIA should be carried out, even where processing was underway prior to the GDPR coming into effect¹.

	DOES THE PROCESS INVOLVE:	YES/NO
1.2.1	A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning individuals or similarly significantly affect individuals.	NO
1.2.2	A systematic monitoring of a publicly accessible area on a large scale.	NO
1.2.3	The Data Protection Commission has determined that a DPIA will also be mandatory for the following types of processing operation where a documented screening or preliminary risk assessment indicates that the processing operation is likely to result in a high risk to the rights and freedoms of individuals pursuant to GDPR Article 35(1) : Lists of Types of Data Processing Operations which require a DPIA. <i>(if this hyperlink does not work, use the following url: https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Data-Protection-Impact-Assessment.pdf)</i>	NO

Table 1.4

If 'Yes' to any then you are likely required to carry out a DPIA under [Article 35](#) GDPR.

If 'No', to all then a DPIA may not be required.

¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504>



2. Purpose of the Data Sharing

2.1 Framework

This Data Sharing Agreement sets out the framework for the sharing of personal data between the Parties and defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to one another.

This agreement is required to ensure that any sharing of personal data is carried out in accordance with the GDPR and the Data Sharing and Governance Act 2019, and each Party agrees to be bound by this agreement until such time as the agreement is terminated, or the Party withdraws from the agreement.

The Parties shall not process shared personal data in a way that is incompatible with the relevant purposes and this agreement.

The Parties will ensure that the Data Sharing Agreement remains fit for purpose, accurate and up to date.

The Parties will actively monitor and periodically review the data sharing arrangement to ensure that it continues to be compliant with data protection law, that it continues to meet its objective, that safeguards continue to match any risks posed, that records are accurate and up to date, that there is adherence to the data retention period agreed and that an appropriate level of data security is maintained.

The Parties must address all recommendations made regarding this Data Sharing Agreement by the Data Governance Board.



2.2 Performance of a Function

Where a public body discloses personal data to another public body under this agreement, it shall be for the purpose of the performance of a function of the public bodies mentioned, and for one or more of the following purposes (please select):

No.	DESCRIPTION	Select
I	To verify the identity of a person, where one or more of the public bodies are providing or proposing to provide a service to that person	<input type="checkbox"/>
II	To identify and correct erroneous information held by one or more of the public bodies mentioned	<input type="checkbox"/>
III	To avoid the financial or administrative burden that would otherwise be imposed on a person to whom a service is being or is to be delivered by one or more of the public bodies mentioned where one of mentioned public bodies to collect the personal data directly from that person	<input type="checkbox"/>
IV	To establish the entitlement of a person to the provision of a service being delivered by one or more of the public bodies mentioned, on the basis of information previously provided by that person to one or more of the public bodies mentioned (or another public body that previously disclosed the information to one or more of the public bodies mentioned)	<input type="checkbox"/>
V	To facilitate the administration, supervision and control of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned	<input checked="" type="checkbox"/>
VI	To facilitate the improvement or targeting of a service, programme or policy delivered or implemented or to be delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned	<input checked="" type="checkbox"/>
VII	To enable the evaluation, oversight or review of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned	<input checked="" type="checkbox"/>
VIII	To facilitate an analysis of the structure, functions, resources and service delivery methods of one or more of the public bodies mentioned	<input type="checkbox"/>

Table 2.2

2.3 Details about the Purpose

Provide details of the particular purpose of this Data Sharing Agreement.

PURPOSE	DESCRIPTION
V. To facilitate the administration, supervision and control of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned	The National Care Experience Programme (NCEP) is a programme established by HIQA that seeks to improve the quality of health and social care services in Ireland by asking people about their experiences of care and acting on their feedback. The NCEP is a partnership by HIQA, the Health Service Executive (HSE) and the Department of Health. The NCEP has a suite of surveys that capture the experiences of people using health and social care services. The NCEP has successfully implemented the National Inpatient Experience Survey for five years, the National Maternity Experience Survey in 2020, the National Nursing Home Experience Survey in 2021 and is currently implementing two further surveys; the National Maternity Bereavement Experience Survey and the National End of Life Survey.



<p>VI. To facilitate the improvement or targeting of a service, programme or policy delivered or implemented or to be delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned</p>	<p>The General Register Office (GRO) is the central repository for records relating to births, stillbirths, adoptions, marriages, civil partnerships and deaths in the Republic of Ireland. The GRO operates under the aegis of the Department of Social Protection, who is the lead public body for this data sharing agreement.</p> <p>As lead partner in the NCEP, HIQA is tasked with administrating the survey on behalf of the Department of Health and the HSE. HIQA is the data controller for the National End of Life Survey. In order to administer the questionnaire, HIQA requires personal data from the GRO on both the deceased person and the bereaved relative, hereafter referred to as the “qualified informant”. The personal data that will be shared between the GRO and HIQA to facilitate the survey is limited to the personal data of eligible data subjects and includes:</p> <p>Data of qualified informant:</p> <ul style="list-style-type: none"> • Forename of qualified informant • Surname of qualified informant • Address of qualified informant • Qualification of informant • Relationship of qualified informant to deceased <p>Data of deceased individuals</p> <ul style="list-style-type: none"> • Name of Deceased • Gender of the Deceased • Date of Death of Deceased • Cause(s) of death • Certified cause of death • Place of Death
<p>VII. To enable the evaluation, oversight or review of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of one or more of the public bodies mentioned</p>	<p>The qualified informant (as defined in the Civil Registration Act 2004) is the person that registers the death, the majority of whom are bereaved relatives (a full list of categories of qualified informants can be found here). This survey will be sent to the qualified informant to be completed by themselves or to be passed on to the most relevant person to complete the survey. A national media campaign will be implemented as part of the survey. The qualified informant will be informed about the survey, when registering the death. This is to ensure transparency and to minimise the surprise element of receiving a questionnaire.</p> <p>The personal data shared between the GRO and HIQA will facilitate the administration of the National End of Life Survey as part of the NCEP, which will further facilitate the evaluation of end of life care and inform improvements in health and social care services in accordance with purpose V, VI and VII.</p>

Table 2.3



3. Data to be shared

3.1 Quality

The Parties will take all reasonable steps to ensure that any personal data processed under this agreement is accurate, kept up to date, and that data which is inaccurate, having regard to the purposes for which it was processed, is erased or rectified as soon as is practicable.

Shared personal data shall be limited to the personal data described in [table 3.4](#) to this agreement and will be shared only in the manner as set out in [table 11.2](#) therein. Where a party receiving data is notified of inaccurate data by the data subject, this party is obliged to notify the disclosing Party/Lead Agency.

3.2 Subject Rights

In so far as the shared personal data is processed by the Party/Parties receiving data, as a data controller, the Party/Parties receiving data will deal with data subjects in their exercising of rights set out in the GDPR, including but not limited to, the right of access, the right of rectification, erasure, restriction of processing and to data portability.

Data subjects have the right to obtain certain information about the processing of their personal data through a data subject access request.

Data subject access requests in relation to data processed by the Party/Parties receiving data will be dealt with by them directly. Data subject access requests in relation to data processed by the Party/Parties disclosing data prior to the transfer will be dealt with by them directly.

3.3 Sharing with Third Parties

The Party/Parties receiving data shall not share the shared personal data with any person who has not been authorised to process such data.

3.4 Detail of the information to be disclosed

Provide details of the personal data set to be disclosed and the detail of any non-personal data.

Note:

If the non-personal data and personal data are linked together to the extent that the non-personal data becomes capable of identifying a data subject then the data protection rights and obligations arising under the GDPR will apply fully to the whole mixed dataset, even if the personal data represents a small part of the set.

	DESCRIPTION
Shared Personal Data	<p>Personal data set to include data of eligible qualified informants and deceased persons.</p> <p>Data of qualified informant: Forename of qualified informant Surname of qualified informant Address of qualified informant Qualification of informant Relationship of qualified informant to deceased</p>



	Data of deceased individuals Name of Deceased Gender of the Deceased Date of Death of Deceased Cause(s) of death Certified cause of death Place of Death
Non-personal Data	NA

Table 3.4



4. Function of the Parties

4.1 Function of the Parties

In table 4.1 below:

- Specify the function of the party disclosing data to which the purpose (as defined in [table 2.3](#)) of the data sharing relates
- Specify the function of the party receiving data to which the purpose (as defined in [table 2.3](#)) of the data sharing relates.

PARTY	FUNCTION
i. GRO(DSP)	The GRO is the State authority with responsibility for the registration and recording of life events such as births, stillbirths, marriages, deaths, adoptions, gender recognition and civil partnerships. The GRO derives its authority from the Civil Registration Act 2004. The GRO maintains the national register of deaths pursuant to Part 5 of the 2004 Act.
ii. HIQA	<p>HIQA was established by the Health Act 2007. Its objective is to “promote safety and quality in the provision of health and personal social services for the benefit of the health and welfare of the public” further to section 7 of the 2007 Act. HIQA will administer the survey on behalf of the NCEP, pursuant to the following functions as set out in section 8 (1) of the 2007 Act:</p> <p><i>(g) to operate such other schemes aimed at ensuring safety and quality in the provision of the services as the Authority considers appropriate;</i></p>

Table 4.1



5. Legal Basis

5.1 Legal Grounds

For the purposes identified in this Data Sharing Agreement the Parties confirm that the sharing and further processing of the defined personal data is based on the legal grounds set out in 5.1.1 and 5.1.2.

5.1.1 Appropriate Legislative Provisions for Sharing

Define the appropriate legal provision for sharing based on the following:

- i. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (GDPR Art 6. 1 (e))

Specify the legal obligation for sharing in the table below.

LEGISLATION	DESCRIPTION
Section 13.2	<p>Data Sharing and Governance Act 2019</p> <p>Section 13(2)</p> <p>A public body may disclose personal data to another public body, in a case in which this section applies to such disclosure, only where—</p> <p>(a) the personal data concerned is disclosed—</p> <p>(i) for the purpose of the performance of a function of the first or second mentioned public body, and</p> <p>(ii) for one or more of the following purposes:</p> <p>(V) to facilitate the administration, supervision and control of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of the first or second mentioned public body;</p> <p>(VI) to facilitate the improvement or targeting of a service, programme or policy delivered or implemented or to be delivered</p>



	<p>or implemented, as the case may be, by, for or on behalf of the first or second mentioned public body;</p> <p>(VII) to enable the evaluation, oversight or review of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of the first or second mentioned public body; </p>
--	---

Table 5.1.1

5.1.2 Appropriate Legislative Provisions for Further Processing

Specify the appropriate legal provision for further processing based on the following:

- ii. |processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (GDPR Art 6. 1 (e)) |



LEGISLATION	DESCRIPTION
<p>5.1.2 (i) Art.6 (1) (e) Section 13 (2)</p>	<p>5.1.2.(i)</p> <p>Art.6 (1) (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller and</p> <p>Data Sharing and Governance Act 2019</p> <p>Section 13 (2) A public body may disclose personal data to another public body, in a case in which this section applies to such disclosure, only where—</p> <p>(a) the personal data concerned is disclosed—</p> <p>(i) for the purpose of the performance of a function of the first or second mentioned public body, and</p> <p>(ii) for one or more of the following purposes:</p> <p>(V) to facilitate the administration, supervision and control of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of the first or second mentioned public body;</p> <p>(VI) to facilitate the improvement or targeting of a service, programme or policy delivered or implemented or to be delivered or implemented, as the case may be, by, for or on behalf of the first or second mentioned public body;</p> <p>(VII) to enable the evaluation, oversight or review of a service, programme or policy delivered or implemented or being delivered or implemented, as the case may be, by, for or on behalf of the first or second mentioned public body.</p>

Table 5.1.2



6. Impetus for Data Sharing

Specify the impetus (the motivation or where benefits will be realised) in relation to the data shared under this agreement.

THE IMPETUS FOR THE DISCLOSURE OF DATA WILL COME FROM:	TICK AS APPROPRIATE
▪ Data subject	<input type="checkbox"/>
▪ Public Body	<input checked="" type="checkbox"/>

Table 6.0



7. Categories of Data Shared

The personal data shared may be in relation to individual data subjects and/or classes of data subjects. Classes of data subject may be defined by the parties involved and some examples might be customers, vendors, suppliers, visitors, etc.

Aggregated data is information gathered and expressed in a summary form for purposes such as statistical analysis, and so is not personal data for the purposes of data protection law and GDPR and is not the same as classes of data subject.

Select from the below table and comment as appropriate.

CATEGORY		COMMENT
Individual Data Subject	<input type="checkbox"/>	The GRO registers deaths in the Republic of Ireland. Deaths are registered by qualified informants (usually the next of kin of the deceased).
	<input checked="" type="checkbox"/>	The GRO will transfer a dataset to HIQA, hereafter referred to as the contact dataset. The contact dataset will contain the names and contact details of eligible qualified informants as well as the following details of the eligible deceased individuals: name, address, date of birth, date of death and cause of death.
Classes of Data Subjects	<input checked="" type="checkbox"/>	The contact dataset will contain details of qualified informants who registered a death and the deceased individuals who died while in a care setting and/or received professional care in the home within a specified period of time

Table 7.0



8. Duration and Frequency

8.1 Duration

The start and end dates of the information transfer:

The Data Sharing Agreement will commence on [01 September 2022] and continue until either one of the parties wants to terminate the agreement.]

8.2 Frequency

Indicate the type of transfer that will be required with a description.

TYPE		DESCRIPTION
Once off	<input type="checkbox"/>	
Frequent/regular updates	<input checked="" type="checkbox"/>	4 contact datasets, containing the data of eligible survey participants, will be transferred for each month of the survey sample period: September, October, November and December 2022 respectively. The transfer will take place between September 2022 and May 2023.
Other frequency	<input type="checkbox"/>	

Table 8.2



9. How data will be processed

9.1 Obligations of the Parties in Respect of Fair and Lawful Processing

Each Party shall ensure that it processes the shared personal data fairly and lawfully. Each will comply with the requirements of the Data Protection Act 2018, GDPR and any legislation amending or extending same, in relation to the data exchanged.

Each Party undertakes to comply with the principles relating to the processing of personal data as set out in Article 5 GDPR, in the disclosing of information under this Data Sharing Agreement.

Both Parties shall, in respect of shared personal data, ensure that they provide sufficient information to data subjects in order for them to understand what components of their personal data the Parties are sharing, the purposes for the data sharing and either the identity of the body with whom the data is shared or a description of the type of organisation that will receive the personal data.

9.2 Description of Processing

Include a description of how the disclosed information will be processed by each receiving party.



DESCRIPTION OF PROCESSING	
HIQA	<p>The GRO registers deaths in the Republic of Ireland. The GRO will transfer the contact dataset, to the data controller (HIQA) via a secure file sharing service, as provided by HIQA. The contact dataset will contain the names and contact details of eligible qualified informants as well as details of deceased individuals such as their date of birth, date of death and cause of death - this information will be used to quality assure the dataset upon receipt by HIQA. The contact dataset will be stored in the EU in a secure encrypted format by a data processor (Behaviour and Attitudes) under contract to HIQA. Access to the contact dataset will be limited to four nominated individuals, who will use the dataset to administer the survey. A print service company, who distributes the survey by post to qualified informants, will receive a partial data file via encrypted email, containing personal data that is the names and addresses of qualified informants. After each print run, the files are electronically deleted using file destruction software. This process is overseen by the data processor's IT Manager. The data processor assigns an eight digit survey code to each qualified informant, which is used to manage their responses to the survey. The eight digit survey codes ensure that survey responses can be managed without linking them to qualified informants' names and addresses and therefore ensure that survey responses are pseudonymised. Once online survey responses are received by the data processor, they are stored on the NCEP dashboard, which is securely stored within the European Union. Survey responses are anonymised upon receipt, meaning that all personal identifiers are removed from the responses. The hardcopy survey responses are returned by qualified informants to the data processor's office where they are 'booked in' and kept under lock and key. They are uploaded to the NCEP dashboard and combined with the online survey responses, which are directly uploaded by qualified informants. Uploading hard copy survey responses involves manually transcribing them. As the hard copy responses are transcribed and uploaded to the NCEP dashboard, their soft copy version is anonymised. The programme maintains and executes a data retention and destruction schedule. All personal data is destroyed following the closure of the survey - the survey is considered to be closed following the last day/date that qualified informants can submit their response to the survey. Digital data held by the data processor is destroyed within six weeks of the survey closing. This includes any data collected from the NCEP Helpline pertaining to the survey, the contact dataset, and any other working files such as opt-out files. Hardcopy survey responses will be destroyed within two months of the survey closing. Anonymised survey responses are retained on the NCEP dashboard indefinitely. Destroying the contact dataset and the hard copy responses completely anonymises the data as re-identification of participants is no longer possible following the implementation of these processes. The destruction of the contact dataset and the hardcopy survey responses by the data processor is overseen by HIQA.</p>

Table 9.2



9.3 Further Processing

- Specify any further processing by the Party or Parties receiving data of the personal data disclosed by the disclosing body under this Data Sharing Agreement.

	SPECIFY FURTHER PROCESSING
[HIQA]	NA

Table 9.3.1



10. Restrictions

Specify any restrictions on the disclosure of information after the processing by the Party or Parties receiving data to the personal data disclosed by the disclosing body under this Data Sharing Agreement. Give a description of the restrictions, if any, which apply to the further disclosure of the information in table 10.0 below.

	RESTRICTIONS ON DISCLOSURE AFTER PROCESSING
[HIQA]	NA

Table 10.0



11. Security Measures

11.1 Security and Training

Both Parties shall adhere to the procedures set out in [table 11.2](#) below, regarding the transfer and receipt of data.

The Party/Parties receiving data agree, in accordance Article 32 of the GDPR, to implement appropriate technical and organisational measures to protect the shared personal data in their possession against unauthorised or unlawful processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the shared personal data transmitted, stored or otherwise processed.

This may include, but is not limited to:

1. Policies, guidelines and procedures governing information security.
2. Password protection for computer access.
3. Automatic locking of idle PCs.
4. Appropriate antivirus software and firewalls used to protect integrity and security of electronically processed data.
5. Unique identifiers for every user with access to data.
6. Employees have access only to personal data required for them to do their jobs.
7. Appropriate security where remote access is allowed.
8. Encryption of data held on portable devices.
9. Data breach procedures.
10. Appropriate physical security.
11. Staff training and awareness.
12. Monitoring of staff accessing data.
13. Controlling physical access to IT systems and areas where paper-based data are stored.
14. Adopting a clear desk policy.
15. Appropriate techniques for destruction of data.
16. Having back-ups of data off-site.

Both Parties shall ensure that the security standards appropriate to the transfer of personal data under this agreement are adhered to.

The Party/Parties receiving data shall ensure that all persons who have access to and who process the personal data are obliged to keep the personal data confidential.

The Party/Parties receiving data shall ensure that employees having access to the data are properly trained and aware of their data protection responsibilities in respect of that data.

Access to the data supplied by the Party disclosing data will be restricted to persons on the basis of least privilege, sufficient to allow such persons carry out their role.

Each Party will keep the data secure and ensure that it is transferred securely in accordance with the procedures of this agreement.



11.2 Security Measures

For the purpose of this agreement, particular regard should be given to the data safeguards outlined in the following sections and subsections:

1. 11.2.1 – Lead Agency/Party Disclosing Data
2. 11.2.2 – Party/Parties Receiving Data
3. 11.2.3 – Data Breaches and Reporting

11.2.1 Lead Agency/ Party Disclosing Data

The following questions should be completed by the Lead Agency/ party disclosing data in the data sharing arrangement.

All questions should be answered in a manner that does not compromise any security measures in place.

11.2.1.1	TRANSMISSION	COMPLIES	DOES NOT COMPLY
	When data is being transmitted from the Lead Agency/party disclosing data to the party/parties receiving data, robust encryption services (or similar) are in use. Please provide details.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		<i>The dataset will be transferred securely using robust encryption services, as outlined in 11.2.2..</i>	

Table 11.2.1

11.2.1.2 – SECURITY STATEMENT	
Give an outline of the security measures to be deployed for transmission of personal data, in a manner that does not compromise those security measures.	
You may also provide details of additional measures in place for the sharing of data that are relevant to this arrangement.	
<i>The dataset will be transferred from the GRO to HIQA, via a secure file sharing platform. The dataset will be encrypted in transit and at rest, that is to say, that the dataset will be encrypted, when uploaded to the secure file sharing platform and upon receipt in HIQA, the dataset will remain in an encrypted format until it has served its purpose and is subsequently destroyed, in line with the NCEP's data retention and destruction schedule.</i>	
11.2.1.3 SECURITY SPECIALIST FOR LEAD AGENCY	YES/NO
Please confirm your security specialist has reviewed this Data Sharing Agreement and that their advice has been taken into consideration.	<input checked="" type="checkbox"/>

Table 11.2.2



11.2.2 Party/Parties Receiving Data

The following questions should be completed by the Party receiving the disclosure of data as part of this Data Sharing Agreement.

Where a 'not applicable' response is included, ensure information is provided as to why.

All questions should be answered in a manner that does not compromise any security measures in place.

11.2.2	PARTY/PARTIES RECEIVING DATA STATEMENTS	COMPLIES	DOES NOT COMPLY	NOT APPLICABLE
11.2.2.1	<p>In relation to the disclosed data - access permissions and authorisations are managed appropriately and periodically revalidated.</p> <p>Please provide details for all non-complying or 'not applicable' statements.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<ul style="list-style-type: none"> ▪ <i>The NCEP have an Access Control Policy. The Access Control Policy defines and limits access to NCEP data in the conduct of its surveys.</i> ▪ <i>The dataset shared between the GRO and the NCEP will be processed in line with this policy. A maximum of four nominated individuals will have access to the data, upon receipt by HIQA. Access will be granted on a role and 'need-to-know' basis, namely to administer the National End of Life Survey. Permissions will be granted to 1) quality assure the dataset upon receipt, to ensure that no ineligible survey participants are included 2) distribute the survey to eligible survey</i> 		



			<p><i>participants and 3) manage opt-outs.</i></p> <p><i>Access to the data will be regularly reviewed, to ensure that only those who need access to perform their duties, as outlined above, will be granted.]</i></p>
<p>11.2.2.2</p>	<p>Appropriate controls are in place if the disclosed data is accessed remotely.</p> <p>Please provide details.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<p>11.2.2.3</p>	<p>A least privileged principle (or similar) is in place to ensure that users are authenticated proportionate with the level of risk associated to the access of the data.</p> <p>Please provide details.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		<ul style="list-style-type: none"> ▪ Data is stored on HIQA-approved networks. If data is accessed by staff offsite, it is done so from secure, password-protected, encrypted, work laptops. Data is not stored 'locally' on a staff member's device. ▪ Audit logging and account lockout is enforced on all devices (including remote devices) used to access the data, via local security settings on servers and firewalls, to restrict unauthorised and or nefarious access to National Care Experience Programme data. ▪ All software and devices issued to staff to carry out the National End of Life Survey are protected by anti-virus software, the security of which is routinely reviewed and patched.] 	
		<ul style="list-style-type: none"> ▪ <i>In line with the National care Experience Programme's Data Access Policy, a maximum of four individuals will have access to the data, upon receipt. These individuals will have been assigned specific</i> 	



		<p><i>responsibilities in relation to processing the data. This includes quality assuring the data, distributing the survey by post based on the details provided in the dataset and managing opt-outs.</i></p> <ul style="list-style-type: none"> ▪ <i>A print service company is used to print and distribute postal copies of the survey to qualified informants. The print service company only receives a partial print file, containing names and address, to perform its functions. Following the distribution of the survey, the partial print file is automatically destroyed.</i> ▪ <i>Access permissions will be regularly reviewed and revoked when access is no longer required, to ensure adherence to the least privileged principle.</i> 		
<p>11.2.2.4</p>	<p>Appropriate controls and policies are in place, which minimise the risk of unauthorised access (e.g. through removable media).</p> <p>Please provide details of the protections in place and how they are managed.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		<ul style="list-style-type: none"> ▪ <i>An Access Control Policy is in place, which defines and limits access to NCEP data this data will only be accessible to designated staff members from nominated password protected, encrypted devices.</i> ▪ <i>Audit logging and account lockout is enforced on devices used to access the data, via local security settings on servers and firewalls, to restrict unauthorised and or nefarious access to National Care Experience Programme data.</i> ▪ <i>All software and devices are protected by anti-virus software, the</i> 		



		<p><i>security of which is routinely reviewed and patched.</i></p> <ul style="list-style-type: none"> <i>The data will be destroyed within six weeks of the survey closing. Any devices that hold data will be securely destroyed.</i> 						
<p>11.2.2.5</p>	<p>Data is encrypted at rest on mobile devices such as laptops and removable media.</p> <p>Please provide details for all non-complying or 'not applicable' statements.</p>	<table border="1"> <tr> <td data-bbox="820 483 995 573" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="995 483 1206 573" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1206 483 1414 573" style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td colspan="3" data-bbox="820 573 1414 1391"> <ul style="list-style-type: none"> <i>The data is encrypted at rest on mobile devices.</i> <i>The data processor is the only entity that holds the encryption key for the data.</i> <i>The data can only be accessed from approved, encrypted devices. Data is stored on HIQA-approved networks, and if accessed by staff offsite, is done so from secure, password-protected, encrypted devices. Data is never stored 'locally' on a staff member's device.</i> </td> </tr> </table>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<ul style="list-style-type: none"> <i>The data is encrypted at rest on mobile devices.</i> <i>The data processor is the only entity that holds the encryption key for the data.</i> <i>The data can only be accessed from approved, encrypted devices. Data is stored on HIQA-approved networks, and if accessed by staff offsite, is done so from secure, password-protected, encrypted devices. Data is never stored 'locally' on a staff member's device.</i> 		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
<ul style="list-style-type: none"> <i>The data is encrypted at rest on mobile devices.</i> <i>The data processor is the only entity that holds the encryption key for the data.</i> <i>The data can only be accessed from approved, encrypted devices. Data is stored on HIQA-approved networks, and if accessed by staff offsite, is done so from secure, password-protected, encrypted devices. Data is never stored 'locally' on a staff member's device.</i> 								
<p>11.2.2.6</p>	<p>There are policies, training and controls in place to minimise the risk that data is saved outside the system in an inappropriate manner or to an inappropriate, less secure location.</p> <p>Please provide details.</p>	<table border="1"> <tr> <td data-bbox="820 1391 995 1514" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="995 1391 1206 1514" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1206 1391 1414 1514" style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td colspan="3" data-bbox="820 1514 1414 1993"> <p><i>The NCEP has an Information Governance Framework, which includes an Access Control Policy, a Security Policy and a Security Processes. The data will be stored in line with these policies, which ensures that:</i></p> <ul style="list-style-type: none"> <i>The data is stored and backed up securely. All data is stored on approved network locations. HIQA as data</i> </td> </tr> </table>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<p><i>The NCEP has an Information Governance Framework, which includes an Access Control Policy, a Security Policy and a Security Processes. The data will be stored in line with these policies, which ensures that:</i></p> <ul style="list-style-type: none"> <i>The data is stored and backed up securely. All data is stored on approved network locations. HIQA as data</i> 		
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
<p><i>The NCEP has an Information Governance Framework, which includes an Access Control Policy, a Security Policy and a Security Processes. The data will be stored in line with these policies, which ensures that:</i></p> <ul style="list-style-type: none"> <i>The data is stored and backed up securely. All data is stored on approved network locations. HIQA as data</i> 								



		<p><i>controller approves the storage location of the data it receives and processes as part of the survey. All staff responsible for data processing are made aware of these locations and survey data are only stored in these locations.</i></p> <ul style="list-style-type: none"> ▪ <i>The data will be stored in an encrypted container on a network approved by HIQA. The data processor is the only entity that holds the encryption key for the data.</i> ▪ <i>The data can only be accessed from approved, encrypted devices. Data is stored on HIQA-approved networks, and if accessed by staff offsite, is done so from secure, password-protected, encrypted laptops. Data is not stored 'locally' on a staff member's device.</i> ▪ <i>Training on the NCEP Information Governance framework is provided to all staff who process NCEP data.</i>
<p>11.2.2.7</p>	<p>Do you have policy in place that protects data from accidental erasure or other loss?</p> <p>Please provide details.</p>	<p><i>As per the NCEP's processes, the dataset will be backed up to a secure cloud computing service. The cloud computing service is stored within the EU. The dataset will be encrypted. The data processor, who administers the survey will be the only entity that has the encryption key to the dataset and therefore the only entity that can access the dataset while in the cloud. </i></p>
<p>11.2.2.8</p>	<p>Is data stored in a secure location only for as long as necessary and then securely erased?</p> <p>Please provide details.</p>	<p><i>Yes, the dataset is stored securely at all times. The dataset will be destroyed in line with the NCEP's data retention and destruction schedule that is within 6 weeks of the survey closing. </i></p>

Table 11.2.3



11.2.2.9 – SECURITY STATEMENT

Give an outline of the security measures to be deployed for the storage and accessing of personal data, in a manner that does not compromise those security measures.

You may also provide details of additional measures in place that are relevant to this arrangement.

The National End of Life Survey is governed by the National Care Experience Programme's Information Governance Framework, which includes a security policy, security processes, access control policy and a data breach management procedure. Data processing is compliant and certified to ISO27001

The Information Governance Framework ensures that:

- *All data is transferred securely, using a secure file sharing service.*
- *All transfers have been approved and formally agreed by HIQA and the GRO in the form of this data sharing agreement.*
- *Upon receipt of the data by HIQA, access to the data is controlled as per the Access Control Policy. As per the policy, only four nominated individuals will have access to this data.*
- *The data is encrypted in transit and at rest.*
- *The data is stored and backed up securely. All data is stored on approved network locations. HIQA as data controller approves the storage location of the data it receives and processes as part of the survey. All staff responsible for data processing are made aware of these locations and survey data are only stored in these locations.*
- *Upon receipt of the data, the data processor is the only entity that holds the encryption key for the data.*
- *The data can only be accessed from approved, encrypted devices. Data is stored on HIQA-approved networks, and if accessed by staff offsite, is done so from secure, password-protected, encrypted laptops. Data is not stored 'locally' on a staff member's device.*
- *The data is password protected. Passwords used to access survey data are stored securely and cannot be saved to web browsers.*
- *Audit logging and account lockout is enforced on devices used to access the data, via local security settings on servers and firewalls, to restrict unauthorised and or nefarious access to National Care Experience Programme data.*



- All servers, software and devices are protected by anti-virus software, the security of which is routinely reviewed and patched.
- To distribute the survey, a partial print file is created, containing the minimal amount of data necessary to distribute a postal survey and will only include the names and addresses of survey participants. The print file is processed securely and immediately destroyed, following the distribution of postal surveys, using file destruction software.
- The data is pseudonymised – the data provided by the GRO and used to distribute the survey will never be matched with survey responses and will be stored separately.
- All staff who process data as part of the National End of Life Survey receive training on the National Care Experience Programme’s Information Governance Framework.
- All staff who process data in the conduct of the National Care Experience Programme, must report any suspected or confirmed data security incidents in line with the National Care Experience Programme Data Breach Management Procedure.
- All data processed as part of the National Nursing Home Experience Survey are destroyed in line with the National Care Experience Programme Data Retention and Destruction Policy and Schedule. Following the closure of the survey, this data is held in digital format only and is electronically destroyed within six weeks of the survey closing. No hard copy version of this data will exist.
- All IT equipment, used in the processing of data, is disposed of securely at end of its life cycle.

11.2.2.10 SECURITY SPECIALIST FOR PARTY/PARTIES RECEIVING DATA	YES/NO
Please confirm the security specialist(s) Party/Parties receiving have reviewed this Data Sharing Agreement and that their advice has been taken into consideration.	YES

Table 11.2.4

11.3 Data Breaches and Reporting

If a personal data breach occurs after the data is transmitted to the Party/Parties receiving data, the Party/Parties receiving data will act in accordance with the Data Protection Commission’s Breach Notification Process and in accordance with GDPR requirements.



12. Retention

Define the retention requirements for the disclosed information for the duration of the Data Sharing Agreement and in the event the agreement is terminated, for:

1. the information to be disclosed and
2. the information resulting from the processing of that disclosed information

INFORMATION TYPE	RETENTION REQUIREMENTS
▪ Information to be disclosed	[The NCEP maintains and executes a data retention and destruction schedule. All personal data is destroyed following the closure of the survey. Digital data held by the data processor is destroyed within six weeks of the survey closing - the survey is considered to be closed following the last day/date that qualified informants can submit their response to the survey. This includes any data collected from the NCEP Helpline pertaining to the survey, the contact dataset, and any other working files such as opt-out files.]
▪ Information resulting from the processing of the data	Hardcopy and online survey responses will be destroyed within two months of the survey closing, following anonymisation. Anonymised surveys responses are retained on the NCEP dashboard indefinitely. Destroying the contact dataset and the hard copy responses completely anonymises the data as re-identification of participants is no longer possible following the implementation of these processes as outlined in table 11.3. above. The destruction of the contact dataset and the hardcopy survey responses by the data processor is overseen by HIQA]

Table 12.0



13. Methods Used to Destroy/Delete Data

Detail how information will be destroyed or deleted at the end of the retention period as defined in the Data Sharing Agreement, for:

- i. the information to be disclosed and
- ii. the information resulting from the processing of that disclosed information

INFORMATION TYPE	DESCRIPTION
1. Information to be disclosed	Electronic files are electronically deleted using file destruction software
2. Information resulting from processing of the data	Electronic files e.g. online responses are deleted using file destruction software. Hard copy survey responses are physically shredded. Destruction of data is overseen by HIQA.

Table 13.0



14. Withdrawal from Agreement

14.1 Procedure

Each Party commits to giving a minimum of 90 days' notice of its intention to withdraw from or terminate this Data Sharing Agreement.

Each Party disclosing personal data pursuant to this Agreement reserves the right to withdraw, without notice, access to such data where that Party has reason to believe the conditions of this Data Sharing Agreement are not being observed. Each Party disclosing data will accept no responsibility for any consequences arising from the exercise of this right.

Where the disclosing Party is subsequently satisfied that the conditions of the Data Sharing Agreement are being observed, access will be restored forthwith.

Where access to shared personal data is withdrawn, the withdrawing Party shall provide to the other Party reasons for that withdrawal as soon as is practicable thereafter. Where there are only 2 Parties, withdrawal by either one shall be considered a termination of the agreement. Where an agreement has multiple Parties and one withdraws, the Lead Agency should update the schedule and inform the other Parties to the agreement.

Where a Data Sharing Agreement expires or is terminated, the Lead Agency shall notify the Minister in writing within 10 days of the withdrawal. The Lead Agency shall also notify the Data Governance Board as soon as practicable after such expiration or termination, as the case may be.

14.2 Severance

If any provision of this agreement (or part of any provision) is found by any court or other authority of competent jurisdiction to be invalid, illegal or unenforceable, that provision or part-provision shall, to the extent required, be deemed not to form part of this agreement, and the validity and enforceability of the other provisions of this agreement shall not be affected.



15. Other Matters

15.1 Variation

No variation of this agreement shall be effective unless it is contained in a valid draft amendment agreement executed by the Parties to this Data Sharing Agreement in accordance with the procedures and requirements set out in Part 9, chapter 2 of the Data Sharing and Governance Act 2019.

15.2 Review of Operation of the Data Sharing Agreement

The Parties shall review the operation of the Data Sharing Agreement on a regular basis, with each such review being carried out on a date that is not more than 5 years from:

1. in the case of the first such review, the date on which the Data Sharing Agreement came into effect, and
2. in the case of each subsequent review, the date of the previous review. A review under s.20(1) shall consider the impact of the technical, policy and legislative changes that have occurred since the date of the previous review under s.20(1).

Where the Parties to the Data Sharing Agreement consider that it is appropriate following completion of a review they shall prepare an amended Data Sharing Agreement to take account of the technical, policy and legislative changes that have occurred since the date of the previous review or the effective date. The amended agreement will be executed by the Parties in accordance with the procedures and requirements set out in Part 9, chapter 2 of the Data Sharing and Governance Act 2019.

15.3 Jurisdiction

This agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the laws of the Republic of Ireland.

15.4 Indemnity

The Party/Parties receiving data shall indemnify and keep indemnified the Party/Parties disclosing data, in full, from and against all claims, proceedings, actions, damages, losses, penalties, fines, levies, costs and expenses, whether direct or indirect and all consequential or indirect loss howsoever arising out of, in respect of or in connection with any breach by the Party/Parties receiving data, including their servants, of data protection requirements.

15.5 Publication

15.5.1 Public Consultation and publishing a Notice

Public Consultation is managed on behalf of the parties by the Data Governance Unit in OGCI0. Each of the proposed parties will be required to publish, on the same date as the consultation, a notice on their website that they are proposing to enter into the DSA. They should state the documents that are accessible to the public and link to their relevant DSA and DPO statements published on the public consultations website. This notice should invite submissions and include the date of publication of the notice.



15.5.2 Publishing Executed DSA

After each of the Data Governance Board recommendations have been addressed by the parties and after this Data Sharing Agreement has been signed by appropriate Authorised Signatories, the Lead Agency in respect of this Data Sharing Agreement shall publish a copy of the final agreement on a website maintained by it as soon as practicable after sending a copy of the agreement to the Data Governance Unit who will accept it on behalf of the Minister.

15.6 Base Registries

In respect of this Data Sharing Agreement, where the personal data disclosed is contained in a Base Registry, the Base Registry owner will take on the role of Lead agency.



16. Schedule A - Data Protection Impact Assessment

If a data protection impact assessment (DPIA) has been conducted in respect of the data sharing to which this Data Sharing Agreement relates, a summary of the matters referred to in [Article 35\(7\)](#) of the GDPR is required to be filled in the table below.

OR

If a data protection impact assessment has not been conducted as it is not mandatory where processing is not “likely to result in a high risk to the rights and freedoms of natural persons” ([Article 35](#) of the GDPR), outline the reasons for that decision in the table below.

DPIA	SUMMARY OF DATA PROTECTION IMPACT ASSESSMENT
<p>Has been conducted [select appropriately]</p>	<p>[To include a summary of the matters referred to in Article 35(7) GDPR]</p> <p>[To include a summary of the matters referred to in Article 35 (7) GDPR]</p> <p>1. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;</p> <p>The GRO registers deaths in the Republic of Ireland. The GRO will transfer a contact dataset to HIQA via a secure file sharing service. The contact dataset will contain the names and contact details of qualified informants as well as details of the deceased individuals such as their date of birth, date of death and cause(s) of death. Upon receipt of the contact dataset, the data controller is responsible for cleaning and quality assuring the contact dataset and using it to administer a postal survey of qualified informants.</p> <p>The contact dataset and other working files (such as opt-out files) will be stored in an encrypted format, which four pre-identified individuals within the data processor will have access to, to administer the survey.</p> <p>The print service company, who distributes the survey to qualified informants, only receives a partial data file via encrypted email, containing personal data, that is the names and addresses of qualified informants. After each print run, the files are electronically deleted using file destruction software. This process is overseen by the data processor’s IT Manager.</p> <p>The data processor assigns an eight digit survey code to each qualified informant, which is used to manage their</p>



	<p>responses to the survey. Online survey responses are received and retained on the NCEP dashboard, which is stored securely within the European Union. They are anonymised upon receipt, meaning that all personal identifiers are removed from the responses. The hardcopy survey responses are returned by qualified informants to the data processor's office where they are 'booked in' and kept under lock and key. They are uploaded to the NCEP dashboard and combined with the online survey responses, submitted directly by qualified informants. Uploading hard copy survey responses involves manually transcribing them. As the hard copy responses are transcribed and uploaded to the NCEP dashboard, their soft copy version is anonymised.</p> <p>The programme maintains and executes a data retention and destruction schedule. All personal data is destroyed following the completion of the survey. Digital data held by the data processor is destroyed within six weeks of the survey closing. This includes any data collected from the NCEP Helpline pertaining to the survey, the contact dataset, and any other working files such as opt-out files. Hardcopy survey responses will be destroyed within two months of the survey closing. Anonymised survey responses are retained on the NCEP dashboard indefinitely.</p> <p>Destroying the contact dataset and the hard copy responses completely anonymises the data as re-identification of qualified informants is no longer possible following the implementation of these processes. The destruction of the contact dataset and the hardcopy survey responses by the data processor is overseen by HIQA.</p> <p>2. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;</p> <p>The contact dataset will be used to implement a survey of end of life care. Survey responses will be used to inform quality improvements in end of life care, policy, legislation, national standards and regulation. A targeted survey of end of life care could not be conducted without processing the information of qualified informants and deceased people.</p>
--	--



	<p>3. an assessment of the risks to the rights and freedoms of data subjects</p> <p>Risk 1: Data quality and potential data breach There is a risk that the eligibility criteria are not applied correctly and that ineligible survey participants subsequently receive, complete and return a survey questionnaire, which would represent a data breach</p> <p>Risk 2: Retention of personal data There is a risk that qualified informant’s data is retained for a period beyond that which is required for the completion of the survey’s objectives. This risk is particular to situations where personal data 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.</p> <p>Risk 3: Responsibilities are undefined or unclear There is a risk that the responsibilities and boundaries for the roles of data controller, data processor and the GRO are not clearly defined or assigned to the numerous parties involved, which may result in non-adherence to processes to manage the privacy and security of qualified informants’ data.</p> <p>Risk 4: Re-identification using pseudonymised data Administrative data (personal information collected to administer the survey, including the contact details of qualified informants and deceased people) is retained until the last pseudonymised survey responses have been processed — within six weeks of the closure of the survey. There is a risk that qualified informants’ contact details could be linked with their pseudonymised survey responses.</p> <p>Risk 5: Transparency There is a risk that qualified informants will not know that they are being included in the survey and may want to opt out of the survey before their data is processed.</p> <p>Risk 6: Participants’ self-disclosure of sensitive information There is a risk that, in answering qualitative, open-ended questions, qualified informants voluntarily disclose personal and or sensitive data which is not required or sought by the survey, which may directly or indirectly identify them. For example, a qualified informant may provide their name and</p>
--	---



	<p>contact details in their survey response and ask to be contacted.</p> <p>In addition, there is a risk that survey response data may be combined with complaints received by service providers, which may intentionally or unintentionally lead to the identification of qualified informants and or others. This risk is particularly pertinent in service providers with lower numbers</p> <p>Risk 7: Personal information solicited by helpdesk of the Freephone number and info@yourexperience.ie</p> <p>There is a risk that staff operating the Freephone helpline and inbox may unnecessarily request personal data when dealing with queries from qualified informants and or members of the public.</p> <p>4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.</p> <p>Risk 1: Data quality and potential data breach</p> <p>The data controller:</p> <ul style="list-style-type: none">▪ provides the GRO with data fields required to ensure that extraneous and or unnecessary data is not included in the contact dataset▪ arranges for the secure transfer of the data. <p>The data processor:</p> <ul style="list-style-type: none">▪ has developed a process to suppress survey responses completed by ineligible survey participants in the event that they are invited to participate and subsequently complete the survey▪ is under contractual obligation to note any suspected or actual data breaches to the NCEP Senior Programme Manager. <p>The GRO:</p> <ul style="list-style-type: none">▪ applies the eligibility criteria▪ transfers the required data fields as requested by HIQA.
--	---



	<p>Risk 2: Retention of personal data</p> <p>The data controller:</p> <ul style="list-style-type: none">▪ has developed a comprehensive information governance framework, which includes the NCEP Retention and Destruction Policy and Schedule▪ has contractual agreements in place with the data processor to ensure the secure retention and destruction of data, in line with the NCEP Retention and Destruction Policy and Schedule▪ supervises the destruction of the data in line with the schedule▪ has contractual agreements in place with the data processor to ensure that the data controller can audit sub-processors▪ has a data sharing agreement in place with the GRO▪ arranges for the secure transfer of qualified informants' data from the GRO to the data processor. <p>The data processor:</p> <ul style="list-style-type: none">▪ implements the record retention and destruction schedule; qualified informants' data and other working files containing personal data are deleted by the data processor within six weeks of the survey closing. The eight character unique survey codes assigned to qualified informants to track survey responses, will also be deleted within six weeks of the survey closing. The hardcopy responses will also be destroyed within two months of the survey closing.▪ oversees the destruction of print files by the sub processor, through a file eraser programme, immediately after the data have served their purpose. <p>The GRO</p> <ul style="list-style-type: none">▪ transfers all data as per the data sharing agreement▪ deletes the contact dataset from its systems after it has been securely transferred to the NCEP. A record will be retained of the Registration ID (only) for all deaths contained in the contact dataset. This document will be password protected and access will be limited to personnel with a business requirement to access the data. <p>Risk 3: Responsibilities are undefined or unclear</p> <p>The data controller has:</p> <ul style="list-style-type: none">▪ put in place a contract with the data processor (which contains a confidentiality agreement), which authorises and
--	---



	<p>defines data-processing activities necessary to administer the survey</p> <ul style="list-style-type: none">▪ put in place a data sharing agreement with the GRO to ensure the secure transfer of qualified informants' data▪ developed an information governance framework, outlining data protection and security specifications agreed with and implemented by the data processor▪ provided training on information governance to the data processor▪ provided training and guidance for the GRO and the data processor, which outlines all roles and responsibilities in transferring data. <p>The data processor</p> <ul style="list-style-type: none">▪ has a data processing agreement in place with any sub processors it contracts, who process personal data in the conduct of the survey. <p>Risk 4: Re-identification using pseudonymised data</p> <p>The data controller:</p> <ul style="list-style-type: none">▪ has a contract in place with the data processor, which stipulates data processing measures▪ has developed a retention and destruction policy and schedule▪ supervises the destruction of the data in line with the schedule▪ ensures that the contract dataset and survey responses are pseudonymised▪ ensures the survey responses are anonymised, by assigning anonymisation criteria. <p>The data processor securely processes the following categories of data:</p> <ul style="list-style-type: none">▪ Personal data of qualified informants. This data is stored securely by the data processor and encrypted in transit and at rest. This data and any other working files are destroyed within six weeks of the survey closing.▪ Survey responses (those submitted online and hard copy survey responses uploaded by the data processor) are stored on the NCEP Dashboard, which is stored securely within the European Union. Survey responses are anonymised in line with the NCEP's anonymisation criteria.
--	--



	<p>Hardcopy survey responses are held by the data processor in a locked and secure location and are destroyed at the end of the survey cycle.</p> <ul style="list-style-type: none">▪ Print files are deleted immediately after they have served their purpose. After each print run, the files are electronically deleted using file destruction software. This process is overseen by the IT Manager in the data processor. <p>The data processor manages access to the contract dataset, the survey responses and any other personal data it holds; access is managed on a role and 'a need-to-know basis' and access rights are reviewed on a regular basis.</p> <p>Risk 5: Transparency The data controller:</p> <ul style="list-style-type: none">▪ carries out the survey in the public interest, in accordance with Article 6 (1) (e) and 9 (2) (i) of the GDPR and uses the results of the survey to inform quality improvements in end of life care▪ has put a process in place to ensure that qualified informants are informed about the survey, when registering the death▪ facilitates qualified informants in opting out of the survey, if they do not wish to participate▪ implements a national media campaign, to ensure that qualified informants are duly informed about the survey▪ facilitates qualified informants in enacting their rights under the GDPR, such as submitting a data subject access request and having their data destroyed▪ has developed material, such as an information letter and participant information leaflet to be included with the postal survey invitation▪ ensures that all communication for public dissemination is accessible and adheres to NALA guidelines, including cognitively testing the survey tool▪ provides details of its data-processing activities and information governance on www.yourexperience.ie▪ publishes the results of the survey and corresponding quality improvement plans on www.yourexperience.ie. <p>Risk 6: Participants' self-disclosure of sensitive information The data controller:</p> <ul style="list-style-type: none">▪ develops anonymisation criteria for the qualitative survey responses. The criteria ensure that personal identifiers
--	---



	<p>relating to a qualified informant and any other individual are removed and their privacy is protected</p> <ul style="list-style-type: none">▪ applies the anonymisation criteria to all online survey responses on the NCEP dashboard▪ reviews survey response data on the NCEP dashboard before making it available to service providers▪ only makes the data available on the NCEP dashboard at an aggregate, national level and for service providers that receive a minimum of 5 responses. <p>The data processor:</p> <ul style="list-style-type: none">▪ anonymises all hard copy survey responses, when uploading them to the NCEP dashboard. <p>Risk 7: Personal information solicited by helpdesk of the freephone number and info@yourexperience.ie</p> <p>The data controller:</p> <ul style="list-style-type: none">▪ receives emails on encrypted, password-protected devices, stored securely by the data controller▪ does not request personal data from members of the public who contact them▪ deletes all emails at the end of every survey cycle▪ does not record any calls it receives in relation to the survey▪ has developed training and a helpline script for the Freephone number to ensure that the data processor's helpline staff do not request personal information unnecessarily. Operators only take the personal information of people if a specific action is required, however unless callers seek to explicitly opt-out of the survey, ask for a new questionnaire/freepost envelope or opt a deceased qualified informant out of the survey, helpline operators do not request personal data. Operators may ask callers for their survey code, but only if they need to verify the 'participant status' of a caller. <p>The data processor (who manages the helpline during the survey distribution period):</p> <ul style="list-style-type: none">▪ provides training for its helpline staff▪ does not record calls▪ does not request personal data from members of the public who contact them, unless such data is needed to action a caller's request, such as opting qualified informants out of the survey or sending them another copy of the survey. Helpline staff try where possible to complete these actions using the caller's survey code and only record names and addresses, if the survey code is not available
--	---



		<ul style="list-style-type: none"> records all details and or actions emanating from calls in ASKIA software. Once submitted to ASKIA, helpline staff no longer have access to the data. This data can only be accessed by managers in the Computer Assistant Telephone Interviewing (CATI) unit in the data processor. If any personal data is recorded, it is used to action the caller's request e.g. opt-outs and resending surveys. Any data held on the ASKIA platform, that pertains to the National End of Life Survey, is destroyed within six weeks of the survey closing deletes and shreds any records of calls at the end of the survey period. Record only refer to types of calls and other non-personal, operational data.
<p>Has not been conducted [select appropriately]</p>	<input type="checkbox"/>	<p>[NA]</p>

Table 9.0

Note: If the Data Sharing Agreement is amended to reflect a change in the scope, form or content of the data processing, then there is an obligation on the data controllers to consider whether the changes give rise to a high risk to the rights and freedoms of natural persons, such that a DPIA should be carried out.

Under [S.20\(4\)](#) of Data Sharing and Governance Act, an amended draft agreement must be submitted for review to the Data Governance Board in accordance with Part 9, Chapter 2 of the Data Sharing and Governance Act.



17. Schedule B

17.1 Necessary for the Performance of a Function

Outline the reasons why the disclosure of information under this agreement is necessary for the performance of the relevant function and explain why it is proportionate in that context.

HIQA was established by the Health Act 2007. Its objective is to “promote safety and quality in the provision of health and personal social services for the benefit of the health and welfare of the public” further to section 7 of the 2007 Acts. HIQA will administer the Survey on behalf of the National Care Experience Programme pursuant to its functions set out in section 8(1)(g) of the Health Act 2007 that is:

“to operate such other schemes aimed at ensuring safety and quality in the provision of the services as the Authority considers appropriate”

The GRO is the State authority with responsibility for the registration and recording of life events such as births, stillbirths, marriages, deaths, adoptions, gender recognition and civil partnerships. The GRO derives its authority from the Civil Registration Act 2004. The GRO maintains the national register of deaths pursuant to Part 5 of the Civil Registration Act 2004.

The Parties consider the data sharing to be necessary to administer the survey and facilitate the sharing of data in support of the survey. The aim of this Agreement is for the GRO to share the data of qualified informants and the deceased persons with HIQA during the relevant survey period. The transfer of the data of qualified informants and the deceased is necessary to facilitate the distribution of survey forms to the qualified informants. The personal data to be processed for the purposes of the survey is limited to what is absolutely necessary, and much consideration has been given to the principles of data minimisation and the rights of data subjects (qualified informants and the deceased).

The Parties agree that this data sharing will serve to benefit the public interest by facilitating the successful implementation of the survey with the aim of improving standards at a national level in line with the objective and functions of HIQA set out in section 7 and section 8 respectively of the Health Act 2007 as amended. The survey seeks to capture important information on the experience of people using end-of life care, their relatives and friends. This information will be used by policy-makers, health and social care service providers and HIQA to help improve the quality and safety of health and social care services provided to people in Ireland.

The survey will give rise to key insights into the experiences of bereaved persons, their family and friends in terms of their interaction with health and social care providers during the end of life period, improving the quality of services and providing useful data to HIQA and other public bodies. Responses to the survey will be used to inform quality improvements in end of life care, policy, legislation, national standards and regulation. Care has been taken to ensure that the processing of the data is proportionate to the aims and objectives pursued, and that the rights of the persons involved are respected and qualified informants are treated with compassion and sensitivity. A targeted survey of end of life care



could not be conducted, without processing the information of qualified informants and the deceased. The same results cannot be achieved without the processing of their personal data.

It is planned to provide information about the survey and the transfer of data by the GRO to HIQA for the purposes of the survey, to qualified informants in advance of the transfer/processing of their data, in compliance with the GDPR requirements regarding transparency and the right of data subjects to be informed of the processing of their personal data under Article 13/14 of the GDPR. This will take place in the local HSE Civil Registration Office where the death is registered by the qualified informant, in the form of the provision and availability of Frequently Asked Questions (FAQs) and posters, which will sensitively display information about the survey. |



17.2 Safeguards

Summarise the extent to which the safeguards applicable to the data shared under this agreement are proportionate, having regard to the performance of functions by the Parties and the effects of the disclosure on the rights of the data subjects concerned.

3. Data quality and data minimisation:

- The NCEP has developed a Quality Assurance Framework to ensure consistency in the performance of its functions.
- The NCEP has developed a data quality framework to ensure that data quality is consistently applied across the programme. This includes a data quality strategy, a data quality improvement cycle and a data quality assessment tool.
- The contact dataset is collected and processed to distribute the survey to qualified informants. The eligibility criteria will be applied by the GRO and ineligible survey participants will be removed prior to sharing. Following this, the contact dataset will be shared with HIQA and cleaned, quality assured and used to distribute the survey. The contact dataset is not used for any other purpose and destroyed within six weeks of the survey closing.
- The National End of Life Survey questionnaire is reviewed by the data controller's Data Protection Officer, to ensure that any data it gathers are necessary and proportional.
- Survey responses are "pseudoanonymised". This means that survey responses are stored separately to the names and contact details of qualified informants.
- Survey responses are anonymised upon receipt. All personal data that has the potential to identify an individual, including the qualified informant, healthcare staff or any other individual, is removed from the responses.

4. Communication of privacy rights to data subjects:

- Qualified informants will be informed of the survey, when registering the death through the display of posters and provision of FAQs.
- In addition, an information leaflet is provided to all qualified informants upon receipt of the survey, where they are a) assured that their rights as data subjects are protected and b) provided with a link to the NCEP webpage (<https://yourexperience.ie/>), which outlines how the NCEP protects the rights of qualified informants.
- The NCEP webpage includes a Statement of Purpose, a Statement of Information Practices, a Data Protection and Confidentiality Policy, a Record Retention and Destruction Schedule and a summary of the DPIA.
- Further information on NCEP Information Governance and data subject's rights is made available on the NCEP's Privacy Notice (<https://yourexperience.ie/privacy-notice/>)

5. Measures undertaken to ensure processors comply with processing directions:

- The data controller and data processor have a contract; the contract stipulates all measures the data processor must take to ensure the secure processing of all survey data for the NCEP.
- The contract stipulates that any changes to data processing activities, as outlined in the contract, must be discussed with and approved by the data controller.
- The data controller has oversight of any contracts and agreements signed between the data processor and any sub-processors responsible for processing NCEP data.
- During the survey implementation phase, a weekly meeting is held between the data controller and the data processor.



- The data controller has developed an information governance framework, outlining all measures in place to securely process NCEP data, which includes policies and procedures formalising the management and processing of NCEP data. This includes a security policy, security processes and an Access Control Policy, which the data processor must adhere to, when processing NCEP data. Training on the framework is provided for staff in the data processor who work with NCEP data.
- The data controller has contractual agreements in place with the data processor to ensure the secure retention and destruction of data, in line with the NCEP Retention and Destruction Policy.
- International transfers outside of the European Union, conducted by the data processor and or sub processor, must be approved by the data controller and must adhere to any stipulations outlined in the contract, including that the transfer of any data must be in accordance with the rules provided by the GDPR.]



18. Schedule C

18.1 List of Parties to this Agreement

Set out the names of all the Parties to the agreement.

As required under [S.21](#) (3)(a), (b) and (c) of the Data Sharing and Governance Act 2019, this Schedule must be updated by the Lead Agency to include any Parties who have joined the agreement by way of an Accession Agreement, and to remove any Party that has withdrawn from the agreement. The Lead Agency must notify the other Parties of any amendments to this Schedule and the Data Governance Board.

- | |
|---|
| <ol style="list-style-type: none">1. Department of Social Protection (Lead Agency)2. Health Information and Quality Authority (HIQA) (Other Party) |
|---|



19. Authorised Signatory

An authorised signatory is required to sign this Data Sharing Agreement after all recommendations made by the Data Governance Board have been addressed and before the Data Sharing Agreement can be executed.

This signatory has the role of accountability for the data sharing defined in this Data Sharing Agreement and holds the post of Principal Officer (equivalent) or above.

The Parties hereby agree to their obligations pursuant to this Data Sharing Agreement for the transfer of personal data as described in this Data Sharing Agreement.

19.1 Lead Agency

LEAD AGENCY			
Signature:		Date:	
Print Name:			
Position held:	[Insert position of Authorised Signatory]		
Email:			
For and on behalf of:	[Insert name of organisation]		

Table 19.0

19.2 Other Party/Parties

OTHER PARTY			
Signature:		Date:	
Print Name:			
Position held;	[Insert position of Authorised Signatory]		
Email:			
For and on behalf of:	[Insert name of organisation]		

Table 19.1

--	--	--	--



Data Protection Officers Statement

This Statement is separate to the Data Sharing Agreement. It is required by law under section 55(1)(d) of the Data Sharing and Governance Act 2019. The Data Protection Officers in each proposed Party must sign and complete this statement before the Data Sharing Agreement is submitted to the Data Governance Unit for Public Consultation and again at execution stage. This statement will be published on a public website.

The Data Protection Officers in each proposed Party to this Data Sharing Agreement must ensure that they:

- have reviewed the proposed agreement, and
- are satisfied that compliance by the proposed Parties with the terms of the proposed agreement would not result in a contravention of data protection law,
- are satisfied that the agreement is consistent with Article 5(1) of the GDPR

The Parties hereby agree to their obligations pursuant to this Data Sharing Agreement for the transfer of personal data as described in this Data Sharing Agreement.

Lead Agency DPO Statement

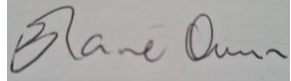
LEAD AGENCY DATA PROTECTION OFFICERS STATEMENT			
I have reviewed the proposed agreement			<input checked="" type="checkbox"/>
I am satisfied that compliance by the proposed Parties with the terms of the proposed agreement would not result in a contravention of data protection law			<input checked="" type="checkbox"/>
I am satisfied that the agreement is consistent with Article 5(1) of the General Data Protection Regulation			<input checked="" type="checkbox"/>
Signature:		Date:	21/07/2022
Print Name:	Elaine Quinn		
Position:	Data Protection Officer		
Email:	DPO@welfare.ie		
For and on behalf of:	[Department of Social Protection]		

Table 19.2



Other Party/Parties DPO Statement

OTHER PARTY DATA PROTECTION OFFICER STATEMENT	
I have reviewed the proposed agreement	<input checked="" type="checkbox"/>
I am satisfied that compliance by the proposed Parties with the terms of the proposed agreement would not result in a contravention of data protection law	<input checked="" type="checkbox"/>
I am satisfied that the agreement is consistent with Article 5(1) of the General Data Protection Regulation	<input checked="" type="checkbox"/>
Signature:	Lydia Buckley
Date:	21/07/22
Print Name:	Lydia Buckley
Position:	Data Protection Officer
Email:	dpo@hiqa.ie
For and on behalf of:	[HIQA]

Table 19.3