#

# http://saltire/my-workplace/communications-and-engagement/Branding-and-marketing/PublishingImages/Pages/brand-guidelines/SG_master_logo_RGB.jpg

# **COVID-19**

# **Information Governance**

# **Rapid Data Protection Assessment v1.4**

If you are starting a COVID-19 related project using personal data, please

**CHECK WITH YOUR LOCAL DATA PROTECTION OFFICE IF THEY HAVE AN EQUIVALENT “RAPID ASSESSMENT” FORM,** otherwise you can use this form and send it to your local data protection/information governance tea, once completed.

Contact details must be available in your local health board website. If you cannot find it, you have contact details for your Data Protection Officer and Caldicott Guardians available here:

<https://www.nhsinform.scot/care-support-and-rights/health-rights/confidentiality-and-data-protection/how-the-nhs-handles-your-personal-health-information#data>

By completing this form and submitting the form to your Data Protection Team you have done your best to comply with the reasonable Information Governance requirement for corporate accountability. You can continue with your project. Your Data Protection Office and/or your IG team will advise you if they have any questions.

NOTE: This template does not negate the need for formal documentation to be completed, such as a Data Protection Impact Assessment, or an Information / Data Sharing Agreement. These documents will be completed accordingly and at an appropriate time. Your Data Protection/Information Governance Team will advise accordingly based on this form.

**Key Principles to remember:**

* **Data Protection legislation does not prohibit the collection and sharing of personal data –** it provides a framework where personal data can be used with confidence that individual’s privacy rights are respected.
* The starting point is to **consider the risks and the potential harm that may arise if we do not share information.**
* Always ensure that the objective can be achieved by sharing the **minimal personal data possible.**
* Remember that processing of personal data must be fair, lawful and transparent.
* Ensure that you have **reasonable security measures** in place to protect the personal data you are processing.

**Further guidance:**

Scottish Government IG advice for COVID-19 working – online at:

[www.informationgovernance.scot.nhs.uk/covid-19-information-governance-advice/](http://www.informationgovernance.scot.nhs.uk/covid-19-information-governance-advice/)

Information Commissioners advice on Data Protection and Coronavirus:

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/data-protection-and-coronavirus/

**Once completed, return this form to your data protection team.**

1. **Requester**

|  |  |
| --- | --- |
| **Name:** |  |
| **Role:** |  |
| **Organisation:** |  |
| **Email:** |  |
| **Telephone number:** |  |

1. **Describe briefly what you want to do and be clear on what is the purpose.**

|  |  |
| --- | --- |
| Brief description of the proposal | Purpose  |
|  |  |

1. **Is this proposal something entirely new for the organisations involved or is an extended use of something that is already in place (e.g. sending messages to patients via SMS) or is a variation or extended use ?**

|  |
| --- |
|  |

1. **Data to be used**

Tick as many categories as required.

Source: e.g. direct collection from the person, an existing dataset or system, etc.

|  |  |  |
| --- | --- | --- |
|  | **Category or type of data** | **Source** |
|  | CHI number |  |
|  | Other identifiers:  |  |
|  | Basic patient demographics (address, contact details, DOB) |  |
|  | Limited and specific health data |  |
|  | Full health records / medical history |  |
|  | Health care provider details (Health board, GP etc.) |  |
|  | COVID-19 Tests |  |
|  | Other (describe) |  |

1. **Technology to be used (tick as many as necessary)**

| **Type** | **Brief details of the technology to be use** |
| --- | --- |
| Dedicated phone App |  |
| Email |  |
| SMS |  |
| Social media |  |
| Website |  |
| Other existing NHS system(s) |  |
| Other existing system elsewhere (e.g. social care system) |  |
| A new system or interface |  |

1. **Organisations involved and their role**

Tick as many as necessary

|  | **Organisation** | **Describe what they will do(role) with the data ?** | **DP (\*)** |
| --- | --- | --- | --- |
|  | *e.g. NSS* | *Collect data about vulnerable people on behalf of Scottish Government, the wider NHS Scotland (health boards, GPs, etc.), print off letters and issue to patients.* |  |
|  | NHS Scotland health board(s). Which ones:  |  |  |
|  | NHS Scotland GPs |  |  |
|  | Health&Care Partnerships (IJBs) |  |  |
|  | Care homes |  |  |
|  | Other in third sector |  |  |
|  | Scottish Government |  |  |
|  | Scottish Local Authorities (e.g. social work) |  |  |
|  | Other Scottish public bodies (e.g. Police Scotland) |  |  |
|  | Another UK health service |  |  |
|  | Another part of central government in the UK nations |  |  |
|  | Other |  |  |
|  | Scottish local authority |  |  |

(\*) In this form, the default position is that the organisation makes decision over the purposes or means by which the data is being used. Some of organisations may only be doing something with the data on behalf of other organisations (e.g. as a service for them), for which they do what they are instructed to. In this case, indicate the organisation is ONLY a data processor by ticking the DP column. Examples of what data processors may do: e.g. print letters, linking and preparing data on behalf of other organisations, collect data on behalf of other organisations, etc.)

1. **Legal basis for processing**

**Current laws do not stop do not stop Government, the NHS or any other health professionals from collecting additional data or sharing personal data to protect against serious threats to public health.**

During this pandemic crisis, is it reasonable to expect that any processing of data required as part of a countermeasures to tackle Coronavirus, will rely one of the following legal basis:

* Processing is necessary in order to protect the **vital interests** of the data subject or of another natural person.
* 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;
* Processing is necessary for the protection of **public health**.

If you feel these assumption doesn’t reflect the circumstances of your proposal, please identify the legal basis your proposal relies on. If you don’t know, please discuss this with your data protection / Information Governance team for advice.

NOTE: We have only included the legal grounds that are likely to apply. If you think your basis is not one of those listed, please add under ‘other’.

Tick/untick the legal basis that best covers the processing under this proposal. You may have more than one legal basis.

|  |  |  |
| --- | --- | --- |
|  | **Basis** | **Guidance** |
| **X** | **Vital interest** | **The processing is necessary to protect someone’s life** |
| **X** | **Public Task** | **The processing is necessary to perform a task in the public interest or for official functions** |
| **X** | **Public Health** | **The processing is necessary for the protection of public health** |
|  | Health or Social Care | The processing is necessary for the provision of health or social care treatment. |
|  | Consent | Individual has given clear consent to process their personal data a specific purpose |
| **X** | **Legal Obligation** | **The processing is necessary to comply with the law** |
|  | Employment, Social Security and Social Protection | The processing is necessary to carry out obligations under employment and social security and social protection law |
|  | Legal obligation | Processing is necessary for compliance with a legal obligation to which NES is subject |
|  | Other |  |

Note: consent is **unlikely** to be the most common legal basis for our processing.

**If there is an legal obligation please indicate what piece of legislation articulates the obligation:**

|  |  |
| --- | --- |
|  | COVID-19 Data Sharing Regulation (Scotland) 2020 |
|  | Other:  |

1. **Is the processing likely to result in high risk ?**

Tick as many as appropriate to reflect the processing of data in your proposal.

|  |  |
| --- | --- |
|  | **Innovative technology**: processing involving the use of unusual technologies, or the novel application of existing technologies (including AI).  |
|  | **Denial of service**: the proposal will involve decisions about an individual’s access to a product, service, opportunity or benefit that is based to any extent on automated decision-making (including profiling) or involves the processing of special category data. |
|  | **Large-scale profiling:**any profiling of individuals on a large scale. |
|  | **Biometric data**  |
|  | **Genetic data**  |
|  | **Data matching:**combining, comparing or matching personal data obtained from multiple sources. |
|  | **Invisible processing:**processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers that compliance with Article 14 would prove impossible or involve disproportionate effort. |
|  | **Tracking:**processing which involves tracking an individual’s geolocation or behaviour, including but not limited to the online environment. |
|  | **Targeting of children or other vulnerable individuals**  |
|  | **Risk of physical harm:**where the processing is of such a nature that a personal data breach could jeopardise the health or safety of individuals. |

1. **Proportionality**

Describe how this proposal is proportionate, considering the purposes, benefits and risks.

|  |
| --- |
|  |

1. **Consultation**

Describe any relevant consultation that has taken place for this proposal.

|  |
| --- |
|  |

1. **Risk assessment (to be completed by IG in conjunction with project sponsor)**

**Risk to the individual (e.g. privacy rights, identity theft, etc.)**

|  |  |
| --- | --- |
| **Description the source of the risk and nature of the potential impact to the individual(s).** | **What are you (or will you be) doing to ensure privacy and confidentiality rights are followed as much as possible ?** |
| **Likelihood of harm to individuals (delete as appropriate):** | Remote / Possible but unlikely / Probably (reasonable change that will happen)  |
| **Severity of harm (delete as appropriate):** | Minimal, significant or severe |
| **Residual risk (delete as appropriate):** | GREEN – AMBER – RED  |

**Risk to the protection of the data (Security)**

|  |  |
| --- | --- |
| **Description the source of the risk and nature of the potential impact to the individual(s).** | **What are you (or will you be) doing to secure the data as much as possible ?** |
| **Likelihood of harm to individuals (delete as appropriate):** | Remote / Possible but unlikely / Probably (reasonable change that will happen)  |
| **Severity of harm (delete as appropriate):** | Minimal, significant or severe |
| **Residual risk (delete as appropriate):** | GREEN – AMBER – RED  |
|

|  |  |  |  |
| --- | --- | --- | --- |
| **PROBABLE** | **GREEN** | **RED** | **RED** |
| **POSSIBLE** | **GREEN** | **AMBER** | **RED** |
| **REMOTE** | **GREEN** | **GREEN** | **GREEN** |
|   | **MINIMAL** | **SIGNIFICANT** | **SEVERE** |

 | **What does ‘significantly affect’ mean?**It is something that has a noticeable impact on an individual and can significantly affect their circumstances, behaviour or choices.For example, a significant effect might include something that affects a person’s financial status, health, reputation, access to services or other economic or social opportunities.Decisions that have general little impact could still significantly affect more vulnerable people. |

1. **DPO and Caldicott Guardian advice**

|  |  |  |
| --- | --- | --- |
| DPO  |  | Date:  |
| Summary of DPO advice: |

|  |  |  |
| --- | --- | --- |
| CALDICOTT GUARDIAN |  | Date:  |
| Summary of Caldicott Guardian advice: |

1. **Review**

|  |  |  |
| --- | --- | --- |
| This DPIA will kept under review by: |  | The DPO should also review ongoing compliance with DPIA |

1. **Sign off**

Each data controller must keep a copy signed off by their corresponding Senior Information Risk Owner or equivalent, as evidence of due diligence.

|  |  |  |
| --- | --- | --- |
| SENIOR INFORMATION RISK OWNER | Add name and signature (electronic signature is acceptable) | Date:  |