Guidance for completing a Data Protection Impact Assessment for national data opt-out processing (v2.2, 19 August 2019)

Introduction

A Data Protection Impact Assessment (DPIA) is used to identify any additional data protection and privacy risks that are introduced by changes to existing or new processing of personal data. Using the "Check for National Data Opt-outs" service, which enables organisations to apply national data opt-outs to their data disclosures, will require changes to existing data processing procedures.

The guidance in this document gives advice on what to consider and, in places, suggested text to use for each section of the DPIA based on the Information Commissioner's Office (ICO) template. Organisations can use another DPIA template as long as it meets the criteria for an acceptable DPIA as set out in the European guidelines, the guidance in this document will still be relevant.

The advice and guidance in this document are specific to the additional data processing required in order to use the Check for National Data Opt-outs service and create data disclosures with national data opt-outs applied. It is assumed that DPIAs, where considered relevant are in already place for any other processing of personal data along with information governance policies, procedures and training for those staff and clinicians who process patient data.

Organisations remain responsible for considering and including any additional information, risks, mitigations which apply to their own processing.

Guidance and advice for DPIA sections

Step 1: Identify the need for a DPIA

Suggested text

"The service to apply national data opt-outs to data disclosures requires additional processing of confidential patient information (CPI). As this is classed as special category data under DPA 2018 and can involve processing data on a large scale and matching to the national opt-out data which comes from a different source it is considered relevant, in line with the guidance on when to complete a DPIA, to undertake a DPIA to understand and mitigate the additional data protection risks this might introduce."

Step 2: Describe the processing

Suggested text

"The national data opt-out was introduced to give patients a choice on how their confidential patient information is used for purposes beyond their individual care.

The information that the opt-out applies to is special category data as it includes information about a patient's health care and/or treatment that has been collected as part of the care we provide for the patient.

Patients can set or change their national data opt-out choice using an online or contact centre service. When a patient sets a national data opt-out it is in held in a repository on the NHS Spine against the patient's NHS number.

In accordance with the patient's wishes and national data opt-out policy, as a health and care organisation located in England, we are required to apply national data opt-outs when applicable to a use or disclosure of confidential patient information for purposes other than the patient's care or treatment.

Applying the opt-out to a data use/disclosure requires that we check, by using the NHS numbers of patients, whether a patient has registered an opt-out before the data is used/disclosed.

To do this a separate list of the NHS numbers in the data that is going to be used/disclosed needs to be created. The list of NHS numbers is then submitted to the Check for National Data Opt-outs service via the secure Message Exchange for Social Care and Health (MESH) messaging service. The Check for National Data Opt-outs service is an external service provided by NHS Digital. The service checks the list of NHS Numbers against a list of opt-outs created from the repository on the NHS Spine, where a match is found it removes the NHS number from the list and then returns an updated list of NHS numbers (with opt-outs removed) back to us via MESH.

We then match the updated list of NHS numbers against our original set of data that was going to be used/disclosed and remove the entire record for those patient records where the NHS numbers match. This creates a 'cleaned' set of data with opt-outs applied that we can then use/disclose."

Note 1: If you have chosen to cache the national data opt-out data for a cohort of patients, (see the Check for National Data Opt-outs licence agreement) you will need to change the description above to recognise that you process a cohort of all your patient NHS numbers through to the Check for National Data Opt-outs service to create your own cached list of NHS numbers that you use for checking against. As part of this you should also include the additional processing that will be required to update the cached data at regular intervals, and to ensure you are correctly applying the national data opt-out for any newly registered patients whose details are in the data disclosure but were not included when the most recent cached list of NHS numbers was created.

Note 2: If you are using a GP system supplied by TPP, EMIS, Vision or Microtest or using one of the other TPP modules to create data to be disclosed then the processing described above will be carried out automatically by the system once you confirm via the system whether national data opt-outs need to be applied. If you are using a system supplied by TPP you will also just need to make sure the cached list being

used has been refreshed. The suppliers of each system will provide more information on the functionality they will provide.

Step 3: Consultation process

Seek advice and review of the DPIA from subject matter experts e.g. information security, information governance, Caldicott Guardian and IT experts. You may also want to consider reviewing with any patient groups. Where you have a Data Protection Officer they should be engaged throughout this process.

Step 4: Assess necessity and proportionality

Suggested text

"In order to respect and apply national data opt-outs in accordance with patient wishes it is necessary to check patient NHS numbers using the Check for National Data Opt-outs service and to process confidential patient information further in order to be able to apply national data opt-outs as described earlier. Only the minimum amount of data required i.e. the NHS number is used to check if a national data opt-out is held.

The legal basis under GDPR and the Data Protection Act 2018 for us to send and receive NHS numbers (considered personal data but not special category data) to and from the Check for National Data Opt-outs service provided by NHS Digital is based on the following:

'Personal Data

- *Article 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'*

In addition to the Article 6 legal basis above, the legal basis under GDPR and the Data Protection Act 2018 to process confidential patient information (considered special category data) in order to apply national data opt-outs is the following:

*'**Special Categories of Personal Data***

- *Article 9(2)(h) allows for processing for management of health and social care based on member state law: which is provided for in the **Data Protection Act 2018**: Schedule 1 Paragraph 2 (2) (f): The processing is necessary for the management of health care systems or service or social care systems or services and is processed by or under the responsibility of a health professional or a social work professional, or by another person who owes a duty of confidentiality under an enactment or rule of law'"*

Note 3: It is suggested that privacy policies and fair processing notices are also updated to indicate how patient NHS numbers are being submitted to the Check for National Data Opt-outs service in order to apply national data opt-outs in accordance with patient wishes.

Step 5: Identify and assess risks

The following identifies some potential risks to consider caused by the additional processing required to apply national data opt-outs to relevant disclosures, these will vary depending upon who is carrying out this additional processing.

Consider the potential impact on patients and any harm or damage that might be caused if the risk materialised and assess the:

Likelihood - remote, possible or probable, Severity - minimal, significant or severe and Overall Rating – low, medium or high

- **Risk 1:** Lack of knowledge or understanding about national data opt-out policy results in national data opt-outs not being applied or being applied incorrectly to a data disclosure.
- **Risk 2:** A 'data processing person', who is not authorised is able to access confidential patient information when creating the list of NHS numbers to send to the service and when applying the list of NHS numbers to a data disclosure.
- **Risk 3:** A 'data processing person' identifies the NHS numbers for patients who have a national data opt-out set, based on the lists sent to and received back from the service.
- **Risk 4:** While the Check for National Data Opt-outs service is being used confidential patient information may be accessed by unauthorised personnel, accidently deleted, destroyed or damaged because the prepared data disclosure is not stored securely.
- **Risk 5:** Where multiple data disclosures are being prepared for release over a short period of time an incorrect 'cleaned' list of NHS numbers from the service may be applied to a data disclosure, resulting in national data opt-outs not being applied correctly.
- **Risk 6:** Where 'cleaned' lists of NHS numbers are being cached if: the cached list is not refreshed in a timely manner this may result in the fair processing window (21 days) for the application of the national data opt-outs from date registered being breached; and/or if the NHS numbers of patients registered since the cache was created are not checked this may result in national data opt-outs not being applied correctly to newly registered patients.
- **Risk 7:** A data processor acting on behalf of the organisation does not apply national data opt-out policy correctly resulting in national data opt-outs not being applied or being applied incorrectly to a data disclosure.

If the national data opt-out is not correctly applied the Information Commissioner's Office have stated this could be treated as a breach of the Data Protection Act (DPA) 2018 requirements for processing to be fair and transparent. If the processing results in unauthorised access to patient data this could be treated as a breach of the DPA 2018 requirements that cover unauthorised or unlawful processing of sensitive personal data.

Step 6: Identify measures to reduce risk

Consider steps to take to effectively reduce and mitigate any risks that have been identified in the previous step. For the potential risks identified in Step 5, the following mitigation actions can be considered to either limit the likelihood of the risk occurring or minimise the impact if it does occur:

- **Risk 1:** Organisations should ensure that relevant staff are aware of and trained in the requirements of the national data opt-out policy. Organisation procedures and policies for existing and new data disclosures and staff training should be updated in order to take account of the national data opt-out. For further help and guidance please see the National data opt-out: compliance implementation guide.

- **Risk 2:** Wherever possible, the processes to create lists of NHS numbers or applying 'cleaned' lists to disclosures should be automated so that there is no need for any additional personnel to have direct access to confidential patient information. If these processes cannot be automated ensure there's a procedure in place so only authorised personnel are involved with this processing and that there are defined and documented roles relevant to this processing.

- **Risk 3:** The process to submit lists of NHS numbers to the service be automated if possible. Otherwise you may consider this to be a low risk that is not treated.

- **Risk 4:** Consider technical security measures (for example, encrypting devices where the data is stored), managing user access rights and ensuring networked areas have the correct view and write permissions.

- **Risk 5:** Ensure organisational policies and procedures and staff training are clear and recommend checks are implemented to make sure the correct 'cleaned' lists are applied to the correct data disclosures. Processes should propose the 'Local id' that is used as part of the Check for National Data Opt-outs service is also used as a unique identifier for each data disclosure so that it is clear the two files relate to each other. If automated processes are in place to apply opt-outs to data disclosures, make sure the system is tested to cope with more than one data disclosure at a time and consider putting checks in place to ensure that all NHS numbers in the 'cleaned list' are actually present in the data disclosure.

- **Risk 6:** Ensure organisational procedures and automated systems where possible are in place so that cached data is refreshed within the time-frames stipulated and newly registered patients not included in previous checks can be identified and their opt-out position confirmed as per the Check for National Data Opt-outs licence agreement. If a scheduled call to the service fails (for example because of a technical connectivity issue with the service) it is recommended that suitable procedures are put in place to halt the processing of data disclosures that require national data opt-outs to be applied until the issues are resolved and the cache is correctly refreshed. Organisations should also consider producing a detailed business continuity plan that captures the key procedures and protocol to be followed in the event of downtime that impacts the processing of personal data. Roles and responsibilities should also be identified to manage business continuity in the event of an incident occurring. For further help and guidance please see the Check for national data opt-outs service licence.

- **Risk 7:** It is the responsibility of the data controller to ensure that national data opt-outs are applied in line with the policy.

  A data processing agreement (DPA) must be in place with the data processor that stipulates how decisions are made on applying national data opt-outs and who is responsible for the processing of those opt-outs along with stipulations on controls over who will have access to the data required to undertake the processing to create the data disclosures. Ideally the processing should be automated as much as is practically possible. It is recommended that you work with your DPO (or equivalent experts in data protection) to detail the data processing activities relevant to how data is collected, processed, stored and what information flows from the data controller to the data processor and that comprehensive and meticulous vetting for a data processor has been carried out. For example, obtain independent compliance certification to confirm the data processor can act effectively within the principles of GDPR compliance.

Step 7: Sign off and record outcomes

The DPIA should be signed off when it is determined that appropriate mitigation actions have been taken for any risks identified or the risk has been determined to be low and no further action needs to be taken. DPIA sign off should be done in conjunction with your Data Protection Officer (where you have one). Processing of data disclosures to apply national data opt-outs should only take place once the DPIA has been agreed.