# Data protection impact assessment (DPIA) | Proxy access to GP online services by care staff

|  |  |
| --- | --- |
| **Name of GP practice** |  |
| **Name of care home** |  |

## Completing a DPIA

Section 35 of the Data Protection Act 2018 mandates the completion of a data protection impact assessment where there is a high risk to the privacy of people from the nature of the information being accessed, and the reasons for it being used.

Completing a DPIA will show:

* you have considered risks to privacy *before* starting to access and use residents’ data
* the actions/mitigations and processes you have put in place in your organisation to reduce risks around accessing sensitive and confidential information

When setting out to complete a data protection impact assessment, do:

* be clear about the reasons for accessing and using the agreed information
* think about the risks to an individual’s privacy
* as well as online information, consider access by care staff to verbal, paper and telephone information used for direct care
* think about how you will you manage any breach of privacy or data security
* remember that the GDPR requires you to ensure transparency of the incident management and accountability processes

## Keeping the DPIA up to date

DPIAs must be reviewed and amended if there are changes to:

* purpose (why)
* manner (how)
* who is involved (people change)

The DPIA template below has been specifically designed for health and social care organisations.

**This template has been produced and signed off by NHSX Information Governance team. It is a recommended best practice template for enabling proxy access by care staff to the online GP records of care home residents. It can be adapted and used for local agreement and sign off.**

|  |  |
| --- | --- |
| **1** | **What is the purpose of accessing and using the personal (and associated health and social care) data?[[1]](#footnote-2)**  The purpose of accessing and using the personal health and social care data is for direct care.  Examples are:   * ordering medication online * viewing test results * viewing discharge information * secure communication between health professionals to receive advice and guidance at the point of care * enabling care information access by the right person at the right time * assessing ongoing needs for care whether acute (from a GP) or secondary care |
| **2** | **Who is accountable, responsible, and controls access to the data by the proxy user?**  GP practices (as data controllers) are accountable and responsible for the access they grant to all information seen by the proxy user. The patient or their representative must have been informed and given consent to the proxy access. Best-interest decisions can be used until such time as legal status is documented and shared, if capacity is being managed. |
| **3** | **Who will be accessing and using the data? Please state the roles in the organisation here**:  Authorised care professionals such as:   * care home manager * deputy manager * clinical lead * administrator * receptionist * senior care staff * activity co-ordinators |
| **4** | **Could you use anonymous data for your purpose/s of accessing this information for your residents? If not, please explain why.**  No, use is for direct care. All the information is needed for specific, named, residents to enable and continue care.   |  |  |  | | --- | --- | --- | | **Item** | **Why** | **Proxy access** | | Allergies and adverse reactions | Resident safety | Yes | | Immunisations | Current status and next due dates | Yes | | Problems and diagnoses | Meet direct care needs | Yes | | Medication | Meet direct care needs and medicines optimisation  Ordering medication | Yes  Yes | | Test results | Meet direct care needs and provide appropriate response with treatment | Yes | | Clinical correspondence | Meet direct care needs and provide appropriate response with treatment  Long-term personalised care planning and support virtually | Yes  Yes | | Appointments | Management of direct long-term care needs | Yes | |
| 5 | **Do you need to use personal and/or health and social care data for the purpose of accessing this information for your residents online? If so, please explain why, and what data items you need to meet that purpose[[2]](#footnote-3).**  Yes, for the direct care for all activities of daily living at various times of the day and night.  Examples are:   * ordering medication online * viewing test results * viewing discharge information * secure communication between health professionals to receive advice and guidance at the point of care * enabling care information access by the right person at the right time * assessing ongoing needs for care whether acute (from a GP) or secondary care |
| **6** | **What steps/actions will you be taking to inform individuals about the use of their personal information online?**  Residents’ information leaflet: letters informing them about changes in the way we share data, why we are doing this and the benefits of this.  Experience shows that secure sharing of information between GPs and care homes**:**   * saves time and money by reducing phone calls across all health and care settings * improves people’s experience by avoiding the need for them to provide the same information to different health and care professionals time and time again * improves health and care professionals’ understanding of an individual’s condition, which personalised treatment planning * improves safety by reducing the need for unnecessary repeated tests * improves safety and experience by making comprehensive and reliable allergy, medication, diagnosis and social circumstance information readily available across all health and care settings * prevents unnecessary admissions to hospital by giving health and care professionals more information about the individual when making their professional decisions * saves time by reducing the need to manually request information * saves money by avoiding duplicate tests or assessments * improves people’s engagement in their own care and adherence with medications and care plans by providing individuals and their carers access to their shared records * supports safeguarding by sharing alerts across multiple care settings |
| **7** | **What is your legal basis for accessing and using residents’ personal data?[[3]](#footnote-4)**  To continue the care needed for residents directly.  The data disclosed will be relevant to the stated purpose(s) of the data sharing agreement and the minimum necessary to achieve the purpose(s).  The personal and special category data to be shared may include name, address, date of birth, NHS number, and a full range of other confidential and sensitive information available to access in the GP record.  When consent to proxy access is being obtained, it is important to make clear the purpose or purposes for which it will be used. If the purpose or purposes change, a new consent will be obtained. |
| **8** | **What is your legal basis for accessing and using an individual's health and/or social care information?[[4]](#footnote-5)**  To continue the care needed for residents directly in accordance with the following statement of basis.  This agreement and process of data relies on the following basis:   * **Article 6 1E**   The lawful basis we rely on to process this personal data is article 6(1)(e) of the GDPR, which allows the processing of personal data when necessary to perform a duty of care   * **Article 9 Paragraph 2H**   To lawfully process special category data, it is necessary to identify both a lawful basis under Article 6 of the GDPR and a separate condition for processing under Article 9. This covers the provision of health or social care or treatment |
| **9** | **If you are using health and social care information that identifies an individual, you will also need to comply with the common law duty of confidentiality. How will you satisfy confidentiality?[[5]](#footnote-6)**  Residents and their representatives have been informed and have consented as part of planned introduction of proxy access for care staff.  All staff have agreed in writing to:   * be accountable and responsible for the information they see in a resident’s record * keep up to date with information governance (IG) * comply with IG policies around data sharing online which complement polices in place for authorised health care professionals who already access this information on paper |
| **10** | **When accessing and using the data, what measures have been taken to ensure the security and safety of data from unlawful, unwarranted or accidental processing by the data processor?**  Passwords are kept safe and changed regularly. Staff know that passwords must not be shared.  IG training and incident reporting processes are in place in the managing organisation(s) which is accountable for incidents and breaches for data security, whether paper or online. |
| **11** | **How will you comply with an individual’s data subject rights (where applicable)?**  All residents or their representatives have been given the option of a conversation to discuss proxy access and understand they can opt out of giving consent to proxy access for their GP record. |
| **12** | **Once the purpose/s of access have been achieved, what will you do with the identifiable information you have used? If you plan on retaining the information, please indicate how long for, the rationale for that period, and what you will do with it at the end of that timescale.**  Information accessed and used is kept in the GP system.  Retaining information may sometimes be required for:   * direct care and personalised care planning * updating care/nursing note or plans * sharing with other health and care professionals that cannot access online information across organisations * providing and enabling professional collaboration to meet the individual resident’s needs with supporting care. This is especially relevant when advanced care planning (ACP) in care homes for end-of-life care (EOL). |
| **13** | **What measures are in place to only use identifiable data for the purposes outlined here?[[6]](#footnote-7)**  GP practices control what information a proxy can see according to local agreements and the wishes of the patient/resident. GP clinical systems audit access to records enabling checks to be made.  Any change to local agreements on levels of access will result in a review of, and amendment to, the data sharing agreement.  The data disclosed will be relevant to the stated purpose(s) of this agreement and the minimum necessary to achieve the purpose(s). |
| **14** | **What potential privacy risks you have identified for the intended use of individual’s data and what actions can you take to reduce these risks to an acceptable level?[[7]](#footnote-8) For any risk that remains high, you must consult with the** **Office of the Information Commissioner** (**ICO) for their advice.**  **If there are any high risks, you must not start to access or use this data until actions have been agreed with the ICO.**  The data disclosed will be relevant to the stated purpose(s) of this agreement and the minimum necessary to achieve the purpose(s).  Potential risks for online proxy access include:   * theft or manipulation of sensitive or private information, such as financial or health records. * computer viruses that can destroy data, damage hardware, cripple systems and disrupt business operations * computer fraud   All organisations should have the above built into their major incident emergency preparedness, response, and resilience (EPPR) plans.  An audit trail is kept in the GP system when a proxy user accesses a patient’s record. It records:   * who accessed which part of the record, and when * what medication was ordered * who authorised or rejected the medication request, and when   Other safeguards include:   * the data sharing agreement between the care home and the GP practice associated with this assessment * all authorised care home staff are up to date with information governance (IG) training and IG requirements * a process is in place to manage any breach of confidentiality or misuse of proxy access * this DPIA   The parties to this agreement commit to put in place, manage and maintain data privacy safeguards appropriate to their circumstances. These will be reviewed regularly to ensure data is not being misused. There are arrangements in place to deal with any person who breaches the terms of the data sharing agreement between the care home and the GP practice. |
| 15 | Signatories to assessment and date  |  |  |  | | --- | --- | --- | | Name of care home (block capitals) |  | | | Name of care home manager/responsible person |  | | | Signature of care home manager/responsible person |  | | | Date |  | | | Name of GP practice manager/responsible person | |  | | | Signature of GP practice manager/responsible person | |  | | | Date | |  | | |

1. If there is more than one purpose (direct and secondary), then these can be listed here, but where necessary, complete a separate DPIA for that purpose. [↑](#footnote-ref-2)
2. You must only access and use the minimum data necessary to achieve that purpose. [↑](#footnote-ref-3)
3. These can be found in Article 6 GDPR. If you are using *Legal Obligation upon a Controller* or *Public Task/Official Authority vested in the Data Controller,* you must specify which piece of legislation or Regulations you are relying upon (including the Section number where relevant). [↑](#footnote-ref-4)
4. These can be found in Article 9 GDPR. [↑](#footnote-ref-5)
5. You will need one of the following: consent, statutory override or substantial Public Interest. [↑](#footnote-ref-6)
6. It is easy for projects/programmes to expand in their aims once they start to see their work coming to fruition. Using information for purposes it was not intended for is a breach of the Data Protection Act 2018. [↑](#footnote-ref-7)
7. Any risk that is still seen as high, even if there are mitigations in place (or if there are no mitigations), must be referred to the ICO. [↑](#footnote-ref-8)