**Data Protection Impact Assessment (DPIA) Template**

**Introduction**

A data protection impact assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project. Once completed, the DPIA should be emailed to Data Security & Protection Team: [dhcft.datasecurityandprotection@nhs.net](mailto:dhcft.datasecurityandprotection@nhs.net)

The General Data Protection Regulations (GDPR) introduces a new obligation to do a DPIA before carrying out types of processing likely to result in high risk to individuals’ interests. If your DPIA identifies a high risk that you cannot mitigate, the DPO will consult with the Information Commissioner’s Office.

A DPIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals.

**When do I need to complete a DPIA?**

You must do a DPIA before you begin any type of processing which is “likely to result in a high risk”. This means that although you have not yet assessed the actual level of risk you need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, a DPIA must be completed if you plan to:

* process special category (including health) or criminal offence data on a large scale; or
* use new technologies;
* use profiling or special category data to decide on access to services;
* match data or combine datasets from different sources;
* collect personal data from a source other than the individual without providing them with a privacy notice (‘invisible processing’);
* track individuals’ location or behaviour;
* profile children or target marketing or online services at them; or
* process data that might endanger the individual’s physical health or safety in the event of a security breach.

If you are unsure whether to complete a DPIA please ask the IG Team to advise.

**Who completes the DPIA?**

The project or service lead should complete the template. Advice can be sought from the Data Security & Protection Team: [dhcft.datasecurityandprotection@nhs.net](mailto:dhcft.datasecurityandprotection@nhs.net)

**DPIA Template** – complete all sections and send to [dhcft.datasecurityandprotection@nhs.net](mailto:dhcft.datasecurityandprotection@nhs.net)

|  |  |
| --- | --- |
| Name: |  |
| Job Title: | Data Security & Protection Lead |
| Email address and telephone number: |  |
| Title of project being assessed: | COVID-19 Digital Staff Passports |
|  | |
| **Brief description of the aim / desired outcome / purpose of the project**: | |
| The aim of the project is to enable clinical and non-clinical staff members, during this Coronavirus emergency, to work in other hospitals/clinical settings run by an organisation who is not their current employer without the need for lengthy employment checks or checks with the relevant professional regulator before they begin work – both of which can take time, thereby impacting direct care.  The national IG panel has reviewed the documentation and NHSX national IG lead has confirmed that it raises no IG issues. The following guidance has been issued Digital staff passport - NHSX.  The Digital Staff Passport will utilise an API which connects with local ESR systems, allowing attributes in staff credentials to be automatically populated. This automated process uses a network routing component provided by Cloud Gateway, traffic through this gateway will be encrypted and will therefore not be privacy intrusive. Automating this process significantly mitigates the risk of entering incorrect information by human error.  This information is pushed to the staff members personal or work smart phone, to the Digital Staff Passport App which they have downloaded. A paper staff passport may also be produced.  NHS England and NHS Improvement and NHSX are the originators of the system and Blackpool Teaching Hospitals NHS Foundation Trust host the system on their behalf (and are Data Processors for this system and hold the contract with Microsoft Azure) and it has been trialled with other Trusts in their area during the first wave of COVID.  Evernym and Truu provide components of the technical solution but will not have access to personal data and will not act as Data Processors. Sitekit also provide secondary technical support for the digital passport system. Sitekit will not routinely have access to personal data, but there may be occasions where personal data is shared with Sitekit staff during the course of providing technical support. | |
| **Describe the nature of the processing:** how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. | |
|  | |
| **Describe the scope of the processing:** what is the nature of the data, and does it include special category (e.g. health) or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover? | |
| Data in the passport:  • Basic personal details– name, date of birth, National Insurance number;  • An ID photograph;  • Basic details relating to work status – DBS information, right to work  • information (residency/visa);  • Professional registration details (GMC/NMC/GDC/HPC);  • Basic details relating to the staff member’s current employment –  • employing organisation, job role, staff group, department, start date  • (and fixed term end date, if appropriate), pay band, work email address,  • smartcard number; and,  • Limited healthcare information specifically relating to the staff member’s  • employment – specifically, Occupational Health clearance.  • Each instance of the COVID-19 Digital Staff Passport system will  • also allow an issuer to upload a photograph of the member of staff  • to the system. | |
| **Describe the context of the processing:** what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? | |
| COVID-19 Digital Staff Passports will be used as a temporary measure during the current Coronavirus emergency. Once this emergency has diminished and there is no longer a need for the scheme, all digital passports will be revoked by the creating organisation.  No children data is collected. | |
| **Describe compliance and proportionality measures, in particular:** what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers? | |
| The lawful basis for each organisation processing the information outlined about staff working at their organisation can be found in the following GDPR articles:  • 6(1)c – Legal obligation, 6(1)e – Public task;  • 9(2)b – Employment, social security and social protection, 9(2)h – Health or social care,  However, user participation in the COVID-19 Digital Staff Passport scheme is entirely voluntary, and as such, the lawful basis for processing information using the Passport system can be found in the following GDPR articles:  • 6(1)a – Consent  • 9(2)a – Consent  A Privacy Notice will be provided to staff participating in the Passport. | |
|  | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | |  |  |  |
| **Identify and assess risks:** | | | |  |  |  |
| **Describe the source of risk and nature of potential impact on individuals.**  Include associated compliance and corporate risks as necessary. | **Likelihood of harm**  (Remote, Possible or Probable) | **Severity of harm**  (Minimal, Significant or Severe) | **Overall risk**  (Low, Medium or High) | **Action(s) to reduce or eliminate the risk** | **Risk level after mitigation** | **Outcome i.e. mitigation to be implemented or risk accepted.** |
| **Risks to the confidentially of personal data. No. Both Cloud Storage and the app on phones have been penetration tested. Access to the information on the phone is encrypted and password or biometric access to the App.** | Remote | significant | medium | Follow trust policy in relation to Data Security & Protection (staff keeping devices locked) | low | Accept residual risk around human error |
| **Are there any risks to the Integrity of personal data? Integrity is defined as unauthorised or accidental alteration of personal data.**  **No. The data is verified by staff and Workforce at the point it is transferred through the system to the phone.** | Remote | minimal | low |  |  |  |
| **Are there any risks to the Availability of personal data? Availability is defined as unauthorised or accidental loss of access to, or destruction of personal data.**  **No** | Remote | minimal | low |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Sign Off and Outcomes**

|  |  |  |
| --- | --- | --- |
| **Item** | **Name / Date** | **Notes** |
| **Risk mitigation measures approved by:** |  | Integrate actions back in to project plan, with date and responsibility for completion. |
| **Residual risks approved by:** |  | If accepting any residual high risk, consult the ICO before going ahead. |
| **Data Protection Officer (DPO) advice given by:** | DPO 02/12/2021 | DPO should advise on compliance, risks assessed and whether processing can proceed. |
| **Summary of DPO advice:** | | |
| Digital Staff Passport has already been reviewed at a national level via NHSX. Application is to be used across NHS and not just limited to Derbyshire. Appropriate security measures in place and clear legal basis.  Key reference this process is temporary during the pandemic and will be closed down once the COVID emergency ends. As such propose to mirror the COPI notice (Control of Patient Information) time frames. | | |
| **DPO advice accepted or overruled by:** | Approved via Data Security & Protection Committee and SIRO 24/11/2021 | If overruled, you must explain your reasons in the comments below. |
| **Comments:** | | |
|  | | |