logo

Data Protection Impact Assessment (DPIA) Questionnaire for

[PROJECT/SYSTEM NAME OR TITLE OF THE PROCESSING ANALYSED]

[INSERT DATE OF THE ASSESSMENT]

**DOCUMENT CONTROL SHEET**

**Key Information**

|  |  |
| --- | --- |
| **Title** |  |
| **Date Published/ Issued** |  |
| **Date Effective From** |  |
| **Version/ Issue Number** |  |
| **Document Type** |  |
| **Document Status** |  |
| **Author** |  |
| **Owner** |  |
| **Approvers** |  |
| **Contact** |  |
| **File Name** |  |

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Summary of Changes** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Name** | **Designation** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**About the Data Protection Impact Assessment (DPIA)**

The DPIA (also known as privacy impact assessment or PIA) is an assessment tool which is used to identify, assess and mitigate any actual or potential risks to privacy created by a proposed or existing process or project that involves the use of personal data. It helps us to identify the most effective way to comply with our data protection obligations and meet individuals’ expectations of privacy. An effective DPIA will allow us to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. Failing to manage privacy risks appropriately can lead to enforcement action from the Information Commissioner’s Office (ICO), which can include substantial fines. The DPIA is just one specific aspect of risk management, and therefore feeds into the overall risk management processes and controls in our organisation.

A DPIA is not a ‘tick-box’ exercise. Consultation may take a number of weeks to complete, so make sure that key stakeholders are engaged early, and that your project plan allows for this so that you have enough time prior to delivery to iron out any issues.

Carrying out a DPIA is an iterative process. Once complete, a review date within the next 3 years must be set. Should a specific change in purpose, substantial change in service or change in the law occur before the review date, the DPIA must be re-done.

The [ICO code of practice on conducting privacy impact assessments](https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf) is a useful source of advice.

**Is a DPIA required?**

If the process or project that you are planning has one or more the aspects listed below then you must complete a DPIA at an early stage.

|  |  | **YES/NO** |
| --- | --- | --- |
| 1. | The work involves carrying out a ***systematic and extensive evaluation*** of people’s personal details, using ***automated processing (including profiling).*** Decisions that have a ***significant effect*** on people will be made as a result of the processing.  Includes:  Profiling and predicting, especially when using aspects about people’s work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements  Processing with effects on people such as exclusion or discrimination  Excludes:  Processing with little or no effect on people |  |
| 2. | The work involves carrying out ***large scale*** processing of any of the ***special categories*** of personal data, or of ***personal data relating to criminal convictions and offences.***  Includes:   * Racial or ethnic origin data * Political opinions data * Religious or philosophical beliefs data * Trade Union membership data * Genetic data * Biometric data for the purpose of uniquely identifying a person * Health data * Sex life or sexual orientation data * Data which may generally be regarded as increasing risks to people’s rights and freedoms e.g. location data, financial data * Data processed for purely personal or household matters whose use for any other purposes could be regarded as very intrusive   To decide whether processing is ***large scale*** you must consider:   * The number of people affected by the processing, either as a specific number or as a proportion of the relevant population * The volume of data and/or the range of different data items being processed * The duration or permanence of the processing * The geographical extent of the processing activity |  |
| 3. | The work involves carrying out ***large scale*** and ***systematic monitoring*** of a ***publicly accessible area.*** Includes processing used to observe, monitor or control people. |  |
| 4. | The work involves ***matching or combining datasets*** e.g. joining together data from two or more data processing activities performed for different purposes and/or by different organisations in a way that people would not generally expect; joining together data to create a very large, new dataset. |  |
| 5. | The work involves processing personal data about ***vulnerable groups.***  This includes whenever there is a power imbalance between the people whose data are to be used e.g. children, the mentally ill, the elderly, asylum seekers, and the organisation using their personal data. |  |
| 6. | The work involves ***significant innovation*** or use of a ***new technology.*** Examples could include combining use of finger print and face recognition for improved physical access control; new “Internet of Things” applications. |  |
| 7. | The work involves transferring personal data across borders ***outside the*** countries listed in the [ICO website](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/) ?   * EEA countries * Countries with an ‘Adequacy decision’ . You can view an up to date list of the countries which have an adequacy finding on [the European Commission's data protection website](http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm). * covered by the EU-US Privacy Shield framework. check on the [Privacy Shield list](https://www.privacyshield.gov/list) to see whether the organisation has a current certification; or * Covered by Canada’s PIPEDA |  |
| 8. | The work involves processing that will ***prevent people from exercising a right*** or using a service or a contract e.g. processing in a public area that people passing by cannot avoid. |  |

**Step One – Consultation Phase**

Consult with all stakeholders about what you wish to do as early as possible in the process. Stakeholders will normally include:

* Key service staff e.g. those who will be managing the process.
* Technical support, especially if a new system is involved. This may involve the relevant IT supplier.
* Information governance advisors e.g. Caldicott Guardian, Information Security Officer, Data Protection Officer.

Sometimes it will be necessary to consult with service users. This will be particularly relevant if the change in process will change how they interact with our NHS Board, or what information is collected and shared about them.

Early consultation will ensure that appropriate governance and security controls are built into the process as it is being designed and delivered, rather than being ‘bolted on’ shortly before the change is launched.

**Step Two- DPIA drafting**

The responsibility for drafting a DPIA will normally sit with the service area that ‘owns’ the change, however, all stakeholders will have an input. Depending on the nature and complexity of your proposal, more than one service area and/ or Information Asset Owner (IAO) may be the owner(s).

**Step Three- Sign-off**

***[NHS Board may need to also add in here specific, local/ administrative details on how DPIAs should be carried out and recorded in their organisation e.g. links with the Information Asset Register, mailboxes to use etc]***

When a DPIA has been fully completed, it must be submitted for formal review by an appropriate IG professional/ the Data Protection Officer. They will review the DPIA to ensure that all information risks are fully recognised and advise whether appropriate controls are in place. The Data Protection Officer will decide, where the DPIA shows a high degree of residual risk associated with the proposal, whether it is necessary to notify the ICO. It may be necessary to inform and/or involve the Board’s Senior Information Risk Owner (SIRO) as part of this risk assessment and decision-making.

Once reviewed, the DPIA will need to be signed off by the Information Asset Owner(s) (IAOs), normally a head of service.

1. **What are you trying to do and why? - give (or attach separately) a high level summary description of the process, including its nature, scope, context, purpose, assets e.g. hardware, software used, data-flows). Explain the necessity and proportionality of the processing in relation to the purpose(s) you are trying to achieve.**
2. **What personal data will be used?**

| **Categories of individuals** | **Categories of personal data** | **Any special categories of personal data [see Guidance Notes for definition]** | **Sources of personal data** |
| --- | --- | --- | --- |
| *e.g. staff* | *e.g. training details* | *e.g. ethnicity* | *e.g. HR system* |
| *e.g. patients* | *e.g. contact details* | *e.g. health data* | *e.g. provided by patient* |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. **What legal condition for using the personal data is being relied upon? [see Guidance Notes for the relevant legal conditions]**

| **Legal condition(s) for *personal data* [see Guidance Notes]** | **Legal conditions for any *special categories of personal data* [see Guidance Notes]** |
| --- | --- |
|  |  |
|  |  |
|  |  |

1. **Describe how the personal data will be collected, used, transferred and if necessary kept up to date – may be attached separately.**
2. **What information is being provided to the people to whom the data relate to ensure that they are aware of this use of their personal data? – This is the** [**‘right to be informed’**](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/) **and information such as privacy notices may be included as an attachment.**
3. **How will people’s individual rights in relation to the use of their personal data be addressed by this process? (Rights are not applicable to all types of processing, and expert advice on this may be necessary.)**

* [Right of access](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/):
* [Right to rectification](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/):
* [Right to object](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/) (where applicable):
* [Right to restrict processing](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/) (where applicable):
* [Right to data portability](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/) (where applicable):
* [Right to erasure](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/) (where applicable):
* [Rights in relation to automated decision-making and profiling](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/) (where applicable):

1. **For how long will the personal data be kept?- refer to our Document Storage Retention and Disposal Policy for advice**
2. **Who will have access to the personal data?**
3. **Will the personal data be routinely shared with any other service or organisation? – if yes, provide details of data sharing agreement(s) and any other relevant controls. Advice on data sharing requirements is in the** [**Scottish Information Sharing Toolkit**](http://www.informationgovernance.scot.nhs.uk/is-toolkit/)**.**
4. **Will the personal data be processed internally by an internal Data Processor or externally by an external Data Processor e.g. an IT services provider? – [see Guidance Notes for the definition of Data Processor]. Provide details of contractor selection criteria, processing instructions and contract (may be attached separately).**
5. **Describe what *organisational* controls will be in place to support the process and protect the personal data (seek the advice of your Information Security Officer as necessary.)**

| **Type of Control – examples** | **Description** |
| --- | --- |
| Information security and related policy(ies) |  |
| Staff training |  |
| Adverse event reporting and management |  |
| Physical access and authorisation controls |  |
| Environmental controls |  |
| Information asset management including management of backups and asset disposal |  |
| Business continuity |  |
| Data Backup |  |
| *Add others where applicable* |  |

1. **Describe what *technical* controls will be in place to support the process and protect the personal data (seek the advice of your Information Security Officer as necessary).**

| **Type of Control – examples** | **Description** |
| --- | --- |
| System access levels and user authentication controls |  |
| System auditing functionality and procedures |  |
| Operating system controls such as vulnerability scanning and anti-virus/anti-malware software |  |
| Network security such as firewalls and penetration testing |  |
| Encryption of special category personal data |  |
| Cyber Essentials compliance(if applicable) |  |
| System Security Policy (SSP) and Standard Operating Procedures(SOPs) (if applicable/ when available) |  |
| Details of ISO27001/02 accreditation and scope (if applicable) |  |
| *Add others where applicable* |  |

1. **Will personal data be transferred to outside the** [**European Economic Area (EEA)**](https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/) **or countries** [**without an European Commission-designated adequate level of protection**](https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en#dataprotectionincountriesoutsidetheeu)**? – if yes, provide details of the safeguards that will be in place for the transfer(s).**
2. **Describe who has been consulted in relation to this process – e.g. subject matter experts, service providers, service users.**
3. **In light of what is proposed, indicate what level of risk has been identified in relation to the following data protection principles:**

| ***Principle*** | ***Low/ Green*** | ***Medium/ Amber*** | ***High/ Red*** |
| --- | --- | --- | --- |
| Personal data is processed in a fair, lawful and transparent manner |  |  |  |
| Personal data is collected for specific, explicit and legitimate purposes |  |  |  |
| Personal data is adequate, relevant and limited to what is necessary |  |  |  |
| Personal data is accurate, and kept up to date |  |  |  |
| Personal data is kept no longer than necessary |  |  |  |
| Personal data is processed in a manner that ensures adequate security |  |  |  |

1. **Risks and actions identified [see Guidance Notes for more information]. List all that you have identified and ensure that these integrate properly with our NHS Board’s risk management process:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Description** | **Likelihood** | **Consequence** | **Overall Risk rating (LxC)** | **Mitigation/ Actions** | **Residual Risk** | **Risk Owner** | **Date** |
| *Add as many as required* |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

1. **Review and Sign-Off**

|  |  |  |
| --- | --- | --- |
| **Role** | **Advice/ Action/ Sign-Off** | **Date** |
| IG/ Data Protection (DPO) Advice |  |  |
| Information Security Officer Advice (questions 11 and 12) |  |  |
| Others, if necessary e.g. Caldicott Guardian, Senior Information Risk Owner (SIRO) |  |  |
| DPO opinion on whether residual risks need prior notification to the ICO |  |  |
| Information Asset Owner(s) (IAO(s)) Sign Off |  |  |

1. **Recommended Review Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**GUIDANCE NOTES**

**Question 2 - Special category personal data**

The special categories of personal data are specified in Article 9 of the General Data Protection Regulation and include data about:

* racial or ethnic origin
* political opinions
* religious or philosophical beliefs
* trade union membership
* genetic data
* biometric data for the purpose of uniquely identifying a person
* health
* sex life or sexual orientation.

Personal data relating to criminal convictions and offences should be regarded as having the same special nature as those in the categories listed above.

**Question 3 – Legal condition**

It is illegal to process personal data without meeting adequately a legal condition.

For personal data which does not relate to any of the special categories (see definition above) the legal basis for the proposed processing must be one or more from the following list. Please note that ‘data subject’ means the person to whom the personal data relates.

* 6(1)(a) – Consent of the data subject
* 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
* 6(1)(c) – Processing is necessary for compliance with a legal obligation
* 6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person
* 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
* 6(1)(f ) – Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject**.**

In NHS Scotland, in many cases condition 6(1)(e) will be the most relevant.

For personal data which relate to any of the special categories (see definition above) the legal basis for the proposed processing must be one or more from the following list:

* 9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
* 9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
* 9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
* 9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
* 9(2)(e) – Processing relates to personal data manifestly made public by the data subject
* 9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
* 9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
* 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
* 9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
* 9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

In NHS Scotland, in many cases condition 9(2)(h) will be the most relevant.

The Information Commissioner’s Office (ICO) advises that public authorities will find using consent as a legal basis difficult. So if the proposed processing is to use consent as its legal basis you need to indicate why this is necessary and seek the advice of an appropriate IG professional.

**Question 10 – Data Processor**

Article 4 of the General Data Protection Regulation defines a Data Processor as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller. In practice it includes organisations and companies that provide services such as records storage, transport and destruction and IT services, where we ask them to carry out specific tasks using personal data on our behalf. IT suppliers, even if only accessing data/systems for support issues or bug fixes, are legally defined as a Data Processor. Data Processors may only be used to process personal information where they have provided sufficient guarantees to implement appropriate technical and organisational measures to comply with the law.

**Question 16 – Risk Assessment**

**ASSESSING THE LEVEL (GRADE) OF THE RISK**

1. Determine the **Likelihood (L)** of recurrence for the event using **Figure 1** (see below).

When determining the likelihood you should consider:

* The frequency of any previous occurrences e.g. How many times a data breach was reported due to this type of issue (e.g. lost records or records accessed without authorisation) in the last month ? in the last year? In the last 5 years?
* You may need to check the Information Governance, Data Protection and Information Security incidents reported in your organisation in order to assess the likelihood.

Figure 1: Likelihood of Recurrence definitions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Descriptor** | **Remote** | **Unlikely** | **Possible** | **Likely** | **Almost Certain** |
| Likelihood | Can’t believe this event would happen – will only happen in exceptional circumstances  (5-10 years) | Not expected to happen, but definite potential exists – unlikely to occur  (2-5 years) | May occur occasionally, has happened before on occasions – reasonable chance of occurring  (annually) | Strong possibility that this could occur – likely to occur  (quarterly) | This is expected to occur frequently / in most circumstances – more likely to occur than not  (daily / weekly / monthly) |

1. Determine the **Consequence (C) rating** using **Figure 2 (see below)**

Look at **events** that **could lead** to the consequence, **not the consequence itself**

e.g. Examples of **Events:**

* Records lost in transit (e.g. paper records sent by post)
* Information recorded inaccurately or not recorded in the record
* Data not available due to ransom-ware attack
* Data lost due to error in IT systems – no useful backup available.
* Confidential personal data sent by email to wrong addressee
* Confidential personal data made available to external people due to poor role access definition and testing
* New system or changes in a system went live without appropriate change management (new or changes in data processing started without IG approval)

**Examples of Consequences**

* Only 1 data subject affected but significant or extreme consequences

e.g. missed vital treatment as a consequence of information not being issued to the patient or health professional leading to death or major permanent incapacity

* very sensitive data being exposed to people who don’t need to know causes extreme distress (could be patient or staff data)
* Large amount of non-sensitive but personal identifiable data lost in the wind when in transit causing organisational embarrassment in the news for a week
* Staff snooping on neighbours medical records
* Excessive health data shared with social worker (husband under domestic abuse investigation) causing direct threats and stalking.
* Personal health data shared by a charity with private business for commercial/marketing purposes causing unwanted disturbance.
* Reportable data breach to ICO causing monetary penalty.
* Complaint from patient to ICO results in undertaking for better access to health records.
* 1.6 million patients in Google Deepmind affected by the processing
* Compliance Audit recommended
* DC action required
* Undertaking served
* Advisory Visit recommended
* Improvement Action Plan agreed
* Enforcement Notice pursued
* Criminal Investigation pursued
* Civil Monetary Penalty pursued

When considering the consequences of a data breach in your proposed service/system which consequence should you opt for?

Don’t choose the worst case scenario or the most likely scenario, but opt for the **“Reasonably foreseeable, worst case scenario”** where if you got a phone call to tell you it had happened, you wouldn’t be surprised.

Figure 2: Consequence Table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Descriptor** | **Negligible** | **Minor** | **Moderate** | **Major** | **Extreme** |
| **Objectives /**  **Project** | Barely noticeable reduction in scope / quality / schedule of an eHealth innovation (e.g. new system) | Minor reduction in scope / quality / schedule | Reduction in scope or quality, project objectives or schedule | Significant project over-run | Inability to meet project objectives, reputation of the organisation seriously damaged  (e.g. Care Data) |
| **Injury**  **(Physical and psychological) to patient / visitor / staff.**  e.g. issues with data quality, availability or confidentiality with physical or psychological consequence for the data subject. | Adverse event leading to minor injury not requiring first aid  (e.g. data quality issues on instruction to patient re prescription) | Minor injury or illness, first aid treatment required | Agency reportable, e.g. Police (violent and aggressive acts)  Significant injury requiring medical treatment and/or counselling.  e.g. Staff member who attempted suicide, privacy compromised as A&E shared details beyond “need-to-know”. | Major injuries/long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling. | Incident leading to death or major permanent incapacity  (e.g. health records not released on time for making treatment decision causing death or major injury). |
| **Patient Experience**  e.g. poor access to my records or difficulties to exert data protection rights. | Reduced quality of patient experience / clinical outcome not directly related to delivery of clinical care | Unsatisfactory patient experience / clinical outcome directly related to care provision – readily resolvable | Unsatisfactory patient experience / clinical outcome, short term effects – expect recovery <1wk | Unsatisfactory patient experience / clinical outcome, long term effects – expect recovery - >1wk | Unsatisfactory patient experience / clinical outcome, continued ongoing long term effects |
| **Complaints / Claims**  e.g. Complaints due to data protection issues | Locally resolved verbal complaint | Justified written complaint peripheral to clinical care | Below excess claim. Justified complaint involving lack of appropriate care | Claim above excess level. Multiple justified complaints | Multiple claims or single major claim |
| **Service / Business Interruption**  e.g. from constant small interruptions of ICT systems to big Business Continuity issues due to cyberattacks or core data centre being down beyond acceptable levels. | Interruption in a service which does not impact on the delivery of patient care or the ability to continue to provide service | Short term disruption to service with minor impact on patient care | Some disruption in service with unacceptable impact on patient care  Temporary loss of ability to provide service | Sustained loss of service which has serious impact on delivery of patient care resulting in major contingency plans being invoked. | Permanent loss of core service or facility  Disruption to facility leading to significant “knock on” effect |
| **Staffing and Competence**  e.g. Poor data protection, confidentiality and ICT security training | Short term low staffing level temporarily reduces service quality (less than 1 day)  Short term low staffing level (>1 day), where there is no disruption to patient care | Ongoing low staffing level reduces service quality  Minor error due to ineffective training / implementation of training | Late delivery of key objective / service due to lack of staff.  Moderate error due to ineffective training / implementation of training  Ongoing problems with staffing levels | Uncertain delivery of key objective / service due to lack of staff.  Major error due to ineffective training / implementation of training | Non-delivery of key objective / service due to lack of staff.  Loss of key staff.  Critical error due to ineffective training / implementation of training |
| **Financial**  **(including damage / loss / fraud)**  e.g. derived from compensation rights as per DPA, ICO or NIS fines, ransomware, etc. | Negligible organisational / personal financial loss  (£<10k) | Minor organisational / personal financial loss  (£10k-100k) | Significant organisational / personal financial loss  (£100k-250k) | Major organisational / personal financial loss  (£250 k-1m) | Severe organisational / personal financial loss  (£>1m) |
| **Inspection / Audit**  e.g. ICO or NIS interventions | Small number of recommendations which focus on minor quality improvement issues | Recommendations made which can be addressed by low level of management action. | Challenging recommendations that can be addressed with appropriate action plan. | Enforcement action.  Low rating  Critical report. | Prosecution.  Zero rating  Severely critical report. |
| **Adverse Publicity / Reputation**  e.g. media attentions due to data breaches or cybersecurity attacks | Rumours, no media coverage  Little effect on staff morale | Local media coverage – short term. Some public embarrassment.  Minor effect on staff morale / public attitudes. | Local media – long-term adverse publicity.  Significant effect on staff morale and public perception of the organisation | National media / adverse publicity, less than 3 days.  Public confidence in the organisation undermined  Use of services affected | National / International media / adverse publicity, more than 3 days.  MSP / MP concern (Questions in Parliament).  Court Enforcement  Public Enquiry |
| **Privacy** | Negligible harm to the individual arising from disclosure of confidential or sensitive information. | Minor harm to the individual arising from disclosure of confidential or sensitive information.  Uncomfortable situation with no material detrimental effect on the person.  Minor impact on dignity. | Moderate harm to the individual arising from disclosure of confidential or sensitive information  e.g. damage to personal relationships and social standing arising from disclosure of confidential or sensitive information | Major harm to the individual arising from disclosure of confidential or sensitive information  e.g. ID theft with potential adverse effect  to the individual for which the person is likely to recover overtime or significant  loss of personal autonomy  detrimental impact on dignity | Extreme harm to the individual arising from disclosure of confidential or sensitive information  e.g. ID theft with financial loss extreme adverse effect or  losing a job  or  Extreme risk to life or health |

Based on: Australian/New Zealand Standard: Risk Management (AS/NZS4360:2004) Risk Management Standard), (2004) Standards Australia/Standards New Zealand

Clinical Governance and Risk Management Standards (2005), NHS Quality Improvement Scotland

3. Use the risk matrix shown in **Figure 3** below to determine the risk grading for the risk. **L x C =R**

Figure 3: Risk Assessment Matrix

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Likelihood | **Consequence** | | | | |
|  | **Negligible** | **Minor** | **Moderate** | **Major** | **Extreme** |
| **Almost certain** | LR | MR | HR | HR | HR |
| **Likely** | LR | MR | MR | HR | HR |
| **Possible** | VLR | LR | MR | MR | HR |
| **Unlikely** | VLR | LR | LR | MR | MR |
| **Remote** | VLR | VLR | VLR | LR | LR |

In terms of grading risks, the following grades have been assigned within the matrix.

Very Low Risk (VLR)

Low Risk (LR)

Moderate Risk (MR)

High Risk (HR)