**S 4.8 Risks to the Rights and Freedoms of Individuals and mitigating 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:**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk No.** | **Data Protection Principle** | **Description** | **Likelihood** | **Consequence** | **Overall Risk rating (LxC)** | **Mitigation/ Actions** | **Residual likelihood** | **Residual consequence** | **Overall residual risk (LxC)** | **Risk Owner** | **Date** |
| ***1*** | *Personal data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.* | ***Data Loss/corruption (accidental/***  ***intentional)  Data Leakage/ex-filtration – data leaving NHSG/system (accidental/***  ***intentional)*** | Possible | Major | Moderate Risk | * Checks will be carried out with Third Party Orgs on appropriate admin processes and IT technology to handle sensitive information. * Data in NHSG & GP Systems are backed up in accordance with local processes. * Sensitive data in the referral form to the Third sector organisation will be via an encrypted email – from NHS email using [Secure] in subject heading. | Unlikely | Major | Moderate Risk | [Partners of <Insert Name of GP Practice>]  Hugh Bishop, SIRO NHSG |  |
| ***2*** | *Personal data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.* | ***Unauthorised access to personal data by NHSG or GP Staff***  ***(accidental/intentional)*** | Unlikely | Major | Moderate Risk | * Access restricted to NHSG/GP only through separate log-in and two factor authentication. * Access to data governed by user role profiles within the relevant system – principle of least privilege applies. * GP Link Worker data is stored securely in a locked down area of the shared drive * Training and a Standard Operating Procedure will be developed for staff members in both NHSG & Practice involved in the Social Prescribing project. * All NHSG & Practice staff bound confidentiality agreements and employee contracts. * All NHSG and Practice staff receive IG & IS training and is refreshed in line with organisational policies. | Unlikely | Major | Moderate Risk | [Partners of <Insert Name of GP Practice>]  Hugh Bishop, SIRO NHSG |  |
| ***3*** | *Personal data shall be accurate, and where necessary, kept up to date.* | ***System/Application/***  ***Process failure/downtime***  ***(accidental/intentional/***  ***planned)*** | Possible | Major | Moderate Risk | * If Sci-GW is unavailable then referrals will not be sent to GP LW until it is back on-line. * If NHS email is unavailable then referrals will not be sent to GP LW until it is back on-line. * Referrals will not be regarded as urgent therefore they can be sent as soon as the systems are functioning. | Unlikely | Major | Moderate Risk | [Partners of <Insert Name of GP Practice>]  Hugh Bishop, SIRO NHSG |  |
| ***4*** | *Personal data shall be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.* | ***Unauthorised/illegal data sharing – without due diligence/appropriate governance in place/out with bounds of DPIA or other Agreement(s)*** | Possible | Moderate | Moderate Risk | * DPIA in place. * Data sharing between Practice and HB is governed by Joint DC & ISA between GPs and NHSS HB. * Separate ISAs will govern the data sharing between Practice & HB and Third sector organisation. * All NHSG & Practice staff bound confidentiality agreements and employee contracts. | Unlikely | Moderate | Low Risk | [Partners of <Insert Name of GP Practice>]  Hugh Bishop, SIRO NHSG |  |
| ***5*** | *Personal data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.* | ***Referral form with patient data sent to incorrect Third Sector Org.*** | Possible | Major | Moderate Risk | * All breaches will be reported in line with Practice/NHSG procedures. * All NHSG & Practice staff bound confidentiality agreements and employee contracts. * All NHSG and Practice staff receive IG & IS training and is refreshed in line with organisational policies. * Practice and GP LW will have own respective SOPs for sharing data and training will be provided. | Unlikely | Major | Moderate Risk | [Partners of <Insert Name of GP Practice>]  Hugh Bishop, SIRO NHSG |  |
| ***6*** | *Processed lawfully, fairly and in a transparent manner.* | ***Referral form to Third Sector Org reveals patient has a personal connection with a member of Third Sector Org.*** | Possible | Moderate | Moderate Risk | * In the event there is a conflict of interest as part of the Third sector organisation receiving the referral, it is up to the Third sector organisation to manage the conflict of interest. * NHSG and Practice staff will not be aware of a potential conflict of interest. | Unlikely | Moderate | Low Risk | [Partners of <Insert Name of GP Practice>]  Hugh Bishop, SIRO NHSG |  |
| ***7*** | *Processed lawfully, fairly and in a transparent manner.* | ***Data subjects may not be aware of how their data is being processed*** | Possible | Moderate | Moderate Risk | * Patient will be advised of process and requirement to share data between Practice and NHSG, and then NHSG and Third sector organisation during referral discussions. * Privacy Notice drafted and to be made available on Practice & NHSG website. | Unlikely | Moderate | Low Risk | [Partners of <Insert Name of GP Practice>]  Hugh Bishop, SIRO NHSG |  |
| ***8*** | *Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.  Personal data shall be accurate, and where necessary, kept up to date.* | ***Data subjects unable to exercise their individual rights*** | Possible | Moderate | Moderate Risk | Both NHSG & Practice have established procedures to administer data subject rights. | Unlikely | Moderate | Low Risk | [Partners of <Insert Name of GP Practice>]  Hugh Bishop, SIRO NHSG |  |
| ***9*** | *Personal data shall be adequate, relevant and limited to what is necessary* | ***Necessity and proportionality*** | Possible | Moderate | Moderate Risk | * Link Worker will determine what patient information necessary and relevant is shared via the standard referral form to the Third Sector Organisation to support the referral. * Data to be shared with third sector org to be discussed and agreed with patient prior to sharing. | Unlikely | Moderate | Low Risk | [Partners of <Insert Name of GP Practice>]  Hugh Bishop, SIRO NHSG |  |
| ***11*** | *Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.* | ***Retention of records*** | Possible | Moderate | Moderate Risk | * Practice Records are retained in perpetuity. * NHSG Sci-GW referrals are stored in accordance with SG RM CoP. * GP LW records are retained in accordance with Records management code of practice. | Unlikely | Moderate | Low Risk | [Partners of <Insert Name of GP Practice>]  Hugh Bishop, SIRO NHSG |  |
| ***12*** | *Personal data shall be adequate, relevant and limited to what is necessary* | ***Excessive, unnecessary or disproportionate data shared with Third sector organisation*** | Possible | Major | Moderate Risk | * Data to be shared with third sector org to be discussed and agreed with patient prior to sharing. * GP LW referral form designed to only capture relevant information for referral. * Training will be developed for GP LW regarding proportionate information sharing. | Unlikely | Major | Moderate Risk | [Partners of <Insert Name of GP Practice>]  Hugh Bishop, SIRO NHSG |  |

**S 4.8 - 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 | Third sector organisation 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)