Market Street Medical Practice

Data Protection Impact Assessment

Insert Asset/Process Name

This document must be completed for any new / or change in service which pertains to utilise Personal Identifiable Data (PID). It must be completed as soon as the new service / or change is identified.

This process is a mandated requirement on the Information Governance Toolkit and legislation to ensure that privacy concerns have been considered and actioned to ensure the security and confidentiality of the personal identifiable information.

Privacy Law and Data Protection compliance checks are part of the DPIA process – the questions to assess this are included in the proforma.

A glossary of terms is at Appendix A for guidance. Further guidance on specific items can be found on the Information Commissioner's website, www.ico.gov.uk.

Document Control

Date	Version	Comments	Author
May 2018	1	Version 1	Insert details

DPIA Version Control

Date	Version	Comments	Author
	0.1		

Section 1 – Screening Questions

The following questions will assist in determining the processing that is likely to pose a high risk (please see Appendix A for high risk criteria).

If you answer 'yes' to any of these questions then a DPIA is required and you should continue to Section 2.

Will the processing task involve the collection of new data or information about individuals?	☐Yes	☐No
Is the processing on a large scale (looking at the number of individuals, the volume of data, the duration or permanence of the processing activity, the geographical extent of the processing)?	☐Yes	☐No
Will the processing compel individuals to provide information about themselves?	☐Yes	☐No
Will the processing of the data prevent an individual from exercising their rights under the GDPR, or prevent them using a service?	☐Yes	☐No
Is the data of a more sensitive nature – does it fall within the special category of data (GDPR)? For example, health records, criminal records or other information that people would consider to be particularly private.	☐Yes	☐No
Does the data concern vulnerable data subjects?	☐Yes	☐No
Will the processing result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	☐Yes	☐No
Is any decision-making about the individual an automated process?	☐Yes	☐No
Is the processing an evaluation or scoring process including profiling?	☐Yes	☐No
Is the data collected being data-matched or combined with other data?	☐Yes	☐No

Will information about individuals be shared or disclosed to organisations or people who have not previously had routine access to the information?	☐Yes	☐No
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	☐Yes	☐No
Will the processing involve you using new technology or cameras which might be perceived as being privacy intrusive? For example the use of facial recognition or positioning technology in a location where the expectation of privacy may be higher.	☐Yes	☐No
Will the processing require the innovative use of new technology or organisational solutions?	☐Yes	☐No

Section 2 – General Details

System /Process name:		
Objective:		
Background/Introduction: **What/Why is the new system / change in system required?**		
Benefits:		
Constraints:		
Relationships: **(for example, with other Trusts, organisations)**		
Cross reference to other projects:		
Project Manager:	Name:	
	Role:	
	Department:	
	Telephone:	
	Email	
Information Asset Owner: **(All systems/assets must have an**	Name:	
	Role:	

Information Asset Owner (IAO). IAOs are normally the Heads of Departments and report to the SIRO)	Department:	
	Telephone:	
	Email	
Information Asset Administrator: **(All systems / assets must have an Information Asset Administrator (IAA) who reports the IAO as stated above. IAAs are normally System Managers / Project Leads)**	Name:	
	Role:	
	Department:	
	Telephone:	
	Email	
Customers and stakeholders: **Please list any and all involved including both internal and external parties**		

Section 3 – Key Questions

Question	Response	Ref to key req. e.g. IGTK, GDPR etc.
1. Will the system/ project/ process (will now be referred to thereafter as 'asset') contain personal identifiable information or special categories data? If answered 'No' you do not need to complete any further information as DPIA is not required.	☐Yes ☐ No If yes, please specify: ☐ Patient ☐Staff ☐ Other (specify)	GDPR Art 35
2. Please state purpose for the collection of the data. For example, patient treatment, health administration, research, audit, staff administration		GDPR Art 5;6;7;8;9
3. Does the asset involve new privacy–invasive technologies? For example facial recognition, biometrics.	☐ Yes ☐ No If yes, please give details:	GDPR Art 35

4. Please tick the data items that are held in the system **Personal** **Special category**	☐ Name ☐ Address ☐ Post Code ☐ Date of Birth ☐ GP ☐ Consultant ☐ Next of Kin ☐ Hospital (District) No. ☐ Gender ☐ NHS Number ☐ Occupation ☐ National Insurance Number ☐ Political opinion ☐ Sexual orientation/ life ☐ Trade union ☐ Religious/ Philosophical ☐ Genetic / biometric ☐ Racial / Ethnic Origin ☐ Medical History ☐ Treatment dates / Diagnosis ☐ Other (please state here):	GDPR Art 6,9
5. Will the asset collect new personal data items which have not been collected before?	☐ Yes ☐ No	
6. What checks have been made regarding the adequacy, relevance and necessity for the collection of personal and/or special categories of data for this asset?	Provide details below:	
7. Does the asset involve new or changed data collection policies that may be unclear or intrusive?	☐ Yes ☐ No	GDPR Art 35
8. Does the third party/ supplier contracts contain all the necessary Information Governance clauses including information about Data Protection and Freedom of Information? **Data Controller / Processor / joint controllers**	☐ Yes ☐ No ☐ Not applicable Enter Data Controller and Data Processor details	IG TK 110 GDPR Art 26; 28; 30
9. Does the asset comply with privacy laws such as the Privacy and Electronic Communications Regulations 2003 **(see appendix A for definition)**	☐ Yes ☐ No ☐ Not applicable	Privacy Law Check

10. Who provides the information for the asset?	☐ Patient ☐ Staff ☐ Others – Please specify	
11. Please list the Conditions for Processing. **(see appendix A, GDPR Article 6 & 9)**	Article 6: Article 9:	GDPR Art 6; 9
12. Are you relying on individuals (patients/ staff) to provide consent (as above Q11) for the processing of personal or special categories of data?	☐ Yes ☐ No If yes, go to question 13. If no, go to question 14.	GDPR Art 6; 7; 8; 9
13. If yes, how will that consent be obtained and managed? Please state.	Explicit consent ☐ Yes ☐ No	GDPR Art 6; 7; 8; 9
14. If no consent obtained, what is the legal basis for processing. **(see appendix A for definition)**	☐ Children Act 2004 ☐ Mental Capacity Act 2005 ☐ Mental Health Act 1983 ☐ Health and Social Care Act 2012 ☐ Care Act 2014 ☐ NHS Act 2006 ☐ Other (Please specify)	
15. Where required, have individuals been informed of and have they given their consent to all the processing and disclosures?	☐ Yes (explicit) ☐ No ☐ Yes (implicit in leaflets, privacy notice on website) If no, which processing / disclosure have specifically been withdrawn?	IGTK GDPR Art 6; 7; 8; 9
16. Who will have access to the information?	☐ Clinical Staff ☐ Non-Clinical Staff ☐ External – Please specify	
17. How will the information be kept up to date and checked for accuracy and completeness?	Provide details below:	GDPR Art 5(1) (d)

18. Do you intend to send direct marketing messages by electronic means? This includes both live and pre-recorded telephone calls, fax, email, text message and picture (including video)?	☐ Yes ☐ No ☐ Not applicable	Privacy Check
19. If applicable, are there procedures in place for an individual's request to prevent processing for purposes of direct marketing in place?	☐ Yes ☐ No ☐ Not applicable	Privacy Check
20. Is automated decision making used? **If yes, how do you notify the individual?** **Can there be any human intervention if required?**	☐ Yes ☐ No Provide details: ☐ Yes ☐ No	Privacy Check GDPR Art 22
21. Is there a useable audit trail in place for the asset? For example to identify who has accessed a record.	☐ Yes ☐ No Provide details:	IGTK
22. Can the data be easily obtained by the Data Subject upon request? For example Subject Access Requests.	☐ Yes ☐ No	GDPR Art 15
23. Have you assessed the risk that the processing of personal/ special categories of data will not cause any unwarranted damage or distress to the individuals concerned? Complete Risks & Issues at Item 46.	☐ Yes ☐ No If yes, provide details of mitigation: If no, provide reasons for this:	
24. What procedures are in place for the rectifying/ right to be forgotten / restriction / object of data by individual request or court order?	Please state all that apply:	GDPR Art 16; 17; 18; 21
25. What notification process is in place to communicate the rectification/ right to be forgotten / restriction of the	☐ Not Applicable	GDPR Art 19

data? (patients / organisations)		
26. Does the asset involve changing the medium for disclosure for publicly available information in such a way that data becomes more readily accessible than before? (For example, from paper to electronic via the web?)	☐ Yes ☐ No ☐ Not Applicable If yes, please provide details.	
27. What are the retention periods (what is the minimum timescale) for this data? (please refer to the NHS Records Management Code of Practice)	Provide details below:	
28. How will the data be destroyed when it is no longer required?	Provide details below:	IGTK
29. What are the data implications upon termination of contract? For example does the data come back to the Trust?	Provide details below:	IGTK GDPR Art 19
30. Does the asset involve multiple organisations whether public or private sector? Include any external organisations. Also include how the data will be sent/accessed and secured. Portability / security	☐ Yes ☐ No If yes provide details below:	GDPR Art 19; 20 GDPR Art 5(f); 32(2)
31. Where will the information be kept/stored/accessed?	☐ On paper ☐ On a database saved on a network folder/drive ☐ Website ☐ On a dedicated system saved to the network – *system name* ☐ Other – please state below:	GDPR Art 5(f) (e)
32. Will any information be sent off site? **If 'Yes' where is this information being sent**	☐ Yes ☐ No Please provide details:	IGTK 208 & 308
33. Please state by which method	☐ Email ☐ Via NHS Mail	IGTK 208

the information will be transported	☐ Website ☐ Via courier ☐ By hand ☐ Via post – internal ☐ Via telephone ☐ Via post - external ☐ Other – please state below:	& 308
34. Has an Information Sharing Agreement been set up?	☐ Yes ☐ No ☐ Not applicable If yes/no, please provide details:	
35. Is personal and / or special category data being transferred outside the UK?	☐ Yes ☐ No If yes, please provide details:	
36. Are you transferring any personal and / or special category data to a country outside the European Economic Area (EEA)? **If yes, where?**	☐ Yes ☐ No If yes, go to Question 37. If no, go to Question 40.	IGTK 209 GDPR Art 5(f); 44; 45
37. What is the data to be transferred to the non EEA country?		IGTK 209 GDPR Art 44; 45
38. Are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country?	☐ Yes ☐ No Please provide detail:	IGTK 209 GDPR Art 35; 32; 44; 45; 46
39. Have you checked that the non EEA country has an adequate level of protection for data security?	☐ Yes ☐ No Please provide detail:	IGTK 209 GDPR Art 44
40. Provide details of any process maps or information flows. (Embed documents please)		

41. Is there a Standard Operating Procedure (SOP) or Policies in place? (Embed documents please)	☐ Yes ☐ No If yes please provide detail:	
42. Has an IT Information Security assessment been carried out and reported to the Information Asset Owner (IAO)? (Date and Embed documents please)	☐ Yes ☐ No If yes, Date completed:	Risk Ass
43. Is there a contingency plan / backup policy in place to manage the effect of an unforeseen event? (Embed documents please)	☐ Yes ☐ No Please provide detail:	Risk Ass GDPR Art 33; 34
44. Are there procedures in place to recover data (both electronic /paper) which may be damaged through: • **Human error** • **Computer virus** • **Network failure** • **Theft** • **Fire** • **Flood** • **Other disaster**	☐ Yes ☐ No Please provide details and procedure / policy titles below:	Risk Ass
45. Any other relevant information		

46. Risks & Issues **Any identified risks and issues will be managed by the risk/issue owner identified.** **(See Appendix B for scoring rationale)**	☐ Yes ☐ No If yes, list below including any mitigation scoring and ownership

Risk/ Issue	Description	Impact	Mitigation	Score	Owner

47. Is the third party contract/ supplier of the system registered with the Information Commissioner?	☐ Yes ☐ No ☐ Not applicable Data Protection Registration Details:
48. Is the third party contract/ supplier of the system registered with the Information Governance Toolkit?	☐ Yes ☐ No ☐ Not applicable IG Toolkit Details:
49. Is the third party contract/ supplier of the system registered with Companies House?	☐ Yes ☐ No ☐ Not applicable Companies House Details:
50. Is the third party contract/ supplier of the system ISO27001 / CareCERT compliant?	☐ Yes ☐ No Provide evidence
51. Is a System Level Security Policy (SLSP) required?	☐ Yes ☐ No ☐ Not applicable If yes, state date completed and attach:

Evaluation

52. Recommendations (Advice and Guidance)	

Approval

Name: .....

Title: Practice Manager/Senior GP .....

Signature: .....

Date: .....

Approval - High Risk and Large Scale Processing of Special Category Data (if applicable)

Name: .....

Title: Data Protection Officer .....

Signature: .....

Date:

Market Street Medical Practice

Appendix A – Glossary of Terms

Item	Definition
High Risk Criteria	This is the criteria we are working to as high risk. This is in the screening questions or within the DPIA itself at Section 1: A) Are you doing evaluation or scoring (including profiling and predicting) of aspects specific to the data subject? B) Does the processing involve automated decision making that produces significant effect on the data subject? C) Are you performing systematic monitoring of data subjects, including in a publicly accessible area? D) Does the processing involve sensitive data (special categories of data as defined in Article 9 and data regarding criminal offences)? E) Is the data being processed on a large scale? F) Have datasets been matched or combined? G) Does the data concern vulnerable data subjects (as laid out in Recital 75)? H) Is this an innovative use or does it apply technological or organizational solutions (for example, combining use of finger print and facial recognition)? I) Are you transferring data outside the European Union? J) Will the processing itself prevent data subjects from exercising a right or using a service or a contract?
Personal Data	This means data which relates to a living individual (data subject) who can be identified, directly or indirectly, by reference to an identifier such as name, an identification number, location data, and online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person: A) from those data, or B) From those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller. It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual
Special Categories of Data	This means personal data consisting of information as to the: A) racial or ethnic origin of the individual B) the political opinions of the individual C) the religious or philosophical beliefs of the individual D) whether the individual is a member of a trade union E) processing of genetic or biometric data for uniquely identifying an individual

	F) physical or mental health of the individual G) sex life or sexual orientation of the individual
GDPR Article 6 – Lawfulness of Processing Conditions	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) – 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.
GDPR Article 9 – Conditions for Special Categories of Data	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, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
Direct Marketing	This is "junk mail" which is directed to particular individuals. The mail which are addressed to "the occupier" is not directed to an individual and is therefore not direct marketing. Direct marketing also includes all other means by which an individual may be contacted directly such as emails and text messages which you have asked to be sent to you. Direct marketing does not just refer to selling products or services to individuals, it also includes promoting particular views or campaigns such as those of a political party or charity.
Automated Decision Making	Automated decisions only arise if 2 requirements are met. First, the decision has to be taken using personal information solely by automatic means including profiling, which produces legal effects concerning the data subject or similarly affects them. For example, if an individual applies for a personal loan online, the website uses algorithms and auto credit searching to provide an immediate yes / no decision. The second requirement is that the decision has to have a significant effect on the individual concerned.
Profiling	Consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.
International organisation	Means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or

	on the basis of, an agreement between two or more countries.
Information Assets	Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities. Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and agreements, business continuity plans, software and hardware.
SIRO (Senior Information Risk Owner)	This person is an executive who takes ownership of the organisation's information risk policy and acts as advocate for information risk on the Board
IAO (Information Asset Owner)	These are senior individuals involved in running the relevant service/department. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the assets under their control/area.
IAA (Information Asset Administrator)	There are individuals who ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date. These roles tend to be system managers
Explicit Consent	Express or explicit consent is given by the data subject freely given, specific, informed and unambiguous indication of the data subjects wishes, usually orally (which must be documented in the patients case notes) or in writing, to a particular use of disclosure of information.
Anonymity	Information may be used more freely if the subject of the information is not identifiable in any way – this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek consent, general information about when anonymised data will be used should be made available to patients.
Pseudonymisation	Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to

	technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person Patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference.
Information Risk	An identified risk to any information asset that the Trust holds. Please see the Information Risk Policy for further information.
Privacy Invasive Technologies	Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic. Technologies that are inherently intrusive, new and sound threatening are a concern and hence represent a risk
Authentication Requirements	An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks.
Retention Periods	Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can vary the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after the last date on the record. Any decision to keep records longer than 30 years must obtain approval from The National Archives.
Information Governance Alliance (IGA) Records Management NHS Code of Practice	Is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The code of practice contains an annex with a health records retention schedule and a Business and Corporate (non-health) records retention schedule.
General Data Protection Regulation (EU) 2016/679	European legislation (applied in UK law by the Data Protection Bill 2017) on the protection of natural persons with regard to

(GDPR)	the processing of personal data. The Regulation defines the ways in which information about living people may be legally used and handled. The 6 principles of the Regulation state the fundamental principles relating to processing personal data must: • Be processed fairly and lawfully. • Collected for specified, explicit and legitimate purposes. • Be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. • Be accurate and, where necessary, kept up to date. • 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. • Be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. The Regulation also requires that the Data Controller and Data Processor are both able to demonstrate compliance with these principles.
Privacy and Electronic Communications Regulations 2003	These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information.

Market Street Medical Practice

Appendix B – Risk and Issue Scoring Rationale

A risk grading must be decided upon for the task/activity/hazardous situation in question. This should be done taking into account how likely the people at risk are to be exposed to the identified hazards bearing in mind the control measures already in place to eliminate or minimise exposure.
The Trust operates an established risk grading system based on a 1-5 scale for likelihood and consequence, known as the 5 x 5 matrix. Using this scale the lowest risk is graded as 1, and the highest risk is graded as 25. Risks graded 15 or above are considered High Risk and are eligible for consideration onto the Corporate Risk Register. The matrix operates on the following descriptors (adapted from the tool available on the NPSA website **www.npsa.nhs.uk**).

Table 1 – Consequence Scores

Choose the most appropriate domain for the identified risk from the left hand side of the table Then work along the columns in same row to assess the severity of the risk on the scale of 1 to 5 to determine the consequence score, which is the number given at the top of the column.

	Consequence score (severity levels) and examples of descriptors				
	1	**2**	**3**	**4**	**5**
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Impact on the safety of patients, staff or public (physical/psychological harm).	Minimal injury requiring no/minimal intervention or treatment. No time off work.	Minor injury or illness, requiring minor intervention. Requiring time off work for >3 days. Increase in length of hospital stay by 1-3 days.	Moderate injury requiring professional intervention. Requiring time off work for 4-14 days. Increase in length of hospital stay by 4-15 days. RIDDOR/agency reportable incident. An event which impacts on a small number of patients.	Major injury leading to long-term incapacity/disability. Requiring time off work for >14 days. Increase in length of hospital stay by >15 days. Mismanagement of patient care with long-term effects.	Incident leading to death. Multiple permanent injuries or irreversible health effects. An event which impacts on a large number of patients.

	Consequence score (severity levels) and examples of descriptors				
	1	2	3	4	5
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Quality/complaints/audit	Peripheral element of treatment or service suboptimal Informal complaint/inquiry.	Overall treatment or service suboptimal. Formal complaint. Local resolution. Single failure to meet internal standards. Minor implications for patient safety if unresolved. Reduced performance rating if unresolved.	Treatment or service has significantly reduced effectiveness. Formal complaint. Local resolution (with potential to go to independent review). Repeated failure to meet internal standards. Major patient safety implications if findings are not acted on.	Non-compliance with national standards with significant risk to patients if unresolved. Multiple complaints/ independent review. Low performance rating. Critical report.	Totally unacceptable level or quality of treatment/service. Gross failure of patient safety if findings not acted on. Inquest/ombudsman Inquiry. Gross failure to meet national standards.
Human resources/organisational development/staffing/competence	Short-term low staffing level that temporarily reduces service quality (< 1 day).	Low staffing level that reduces the service quality.	Late delivery of key objective/ service due to lack of staff. Unsafe staffing level or competence (>1 day). Low staff morale. Poor staff attendance for mandatory/key training.	Uncertain delivery of key objective/service due to lack of staff. Unsafe staffing level or competence (>5 days). Loss of key staff. Very low staff morale. No staff attending mandatory/ key training.	Non-delivery of key objective/service due to lack of staff. Ongoing unsafe staffing levels or competence. Loss of several key staff. No staff attending mandatory training /key training on an ongoing basis.

	Consequence score (severity levels) and examples of descriptors				
	1	2	3	4	5
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Statutory duty/inspections	No or minimal impact or breach of guidance/ statutory duty.	Breach of statutory Legislation. Reduced performance rating if unresolved.	Single breach in statutory duty. Challenging external recommendations/ improvement notice.	Enforcement action. Multiple breaches in statutory duty. Improvement notices. Low performance rating. Critical report.	Multiple breaches in statutory duty. Prosecution. Complete systems change required. Zero performance rating. Severely critical report.
Adverse publicity/reputation	Rumours. Potential for public Concern.	Local media coverage – short-term reduction in public confidence. Elements of public expectation not being met.	Local media coverage – long-term reduction in public confidence.	National media coverage with <3 days service well below reasonable public Expectation.	National media coverage with >3 days service well below reasonable public expectation. MP concerned (questions in the House). Total loss of public Confidence.
Business objectives/projects	Insignificant cost increase/ schedule slippage	<5 per cent over project budget. Schedule slippage.	5–10 per cent over project budget. Schedule slippage.	Non-compliance with national 10–25 per cent over project budget. Schedule slippage. Key objectives not met.	Incident leading >25 per cent over project budget. Schedule slippage. Key objectives not met.

	Consequence score (severity levels) and examples of descriptors				
	1	2	3	4	5
Domains	**Negligible**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Finance including claims	Small loss. Risk of claim remote.	Loss of 0.1–0.25% of budget. Claim <£10,000.	Loss of 0.25–0.5% of budget. Claim(s) between £10,000 and £100,000.	Objective/Loss of 0.5–1.0% of budget. Claim(s) between £100,000 and £1 million. Purchasers failing to pay on time.	Non-delivery of key objective/ Loss of >1% of budget. Failure to meet specification/ slippage. Loss of contract / payment by results. Claim(s) >£1 million.
Service/business interruption Environmental impact	Loss/interruption of >1 hour. Minimal or no impact on the environment.	Loss/interruption of >8 Hours. Minor impact on Environment.	Loss/interruption of >1 day. Moderate impact on Environment.	Loss/interruption of >1 Week. Major impact on Environment.	Permanent loss of service or facility. Catastrophic impact on Environment.

Table 2 - Likelihood score (L)

What is the likelihood of the consequence occurring? The frequency-based score is appropriate in most circumstances and is easier to identify. It should be used whenever it is possible to identify a frequency.

Likelihood Score	1	2	3	4	5
Descriptor	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
Frequency How often might it/does it happen	This will probably never happen/recur.	Do not expect it to happen/recur but it is possible it may do so.	Might happen or recur occasionally.	Will probably happen/ recur but it is not a persisting issue.	Will undoubtedly happen/recur, possibly frequently.

Table 3 – Risk Scoring = consequence x likelihood (C x L)

		Likelihood				
		1	2	3	4	5
Consequence		Rare	Unlikely	Possible	Likely	Almost Certain
Catastrophic	5	5	10	15	20	25
Major	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Minor	2	2	4	6	8	10
Negligible	1	1	2	3	4	5

Note: the above table can to be adapted to meet the needs of the individual trust. For grading risk, the scores obtained from the risk matrix are assigned grades as follows:

	1 - 3	Very Low Risk
	4 - 6	Low Risk
	8 - 12	Moderate Risk
	15 - 25	High Risk