## Living With Privacy Impact Assessment v6.1 08/12/21

Approved by LW DPO at version 6.1

**The data controller for this service will be the contracting NHS Organisation, as per the license agreement signed for the contract.**

**LW will act as the data processor under the authority of the data controller as per the license agreement signed for the contract.**

|  |  |
| --- | --- |
| Question | **Response** |
| 1. Will the system/project/process (will now be referred to thereafter as ‘asset’) contain personal identifiable data or special categories (sensitive) data?   If answered ‘No’ you do not need to complete any further information as DPIA is not required. | No Yes  If yes, please specify:  Patient  Staff  Other (specify)  Health organisation user details are held |
| 1. Please state purpose for the collection of the data:   e.g. patient treatment, health administration, research, audit, staff administration, service evaluation | Patient treatment |
| 1. Does the asset involve new privacy–invasive technologies?   (e.g. SIRI, Alexa, Smart TVs, bodycameras)  (Refer to your risk assessment) | Yes  No, but we use cookies see below  If yes, please give details:  We may collect information about the patient device, including where available IP address, operating system version, and device type for system administration and for the purposes of analysing usage patterns. This information does not include personally identifiable information about the patient, but they are unique to each user so that we are able to distinguish between users.  We may use analytics services provided by [**Firebase**](https://firebase.google.com/) and [**Fabric**](https://get.fabric.io/) to collect and analyse usages statistics within the App.  The information we collect will help us to improve the App and to deliver a better and a more personalised service to users. It enables us:  To estimate our audience size and usage pattern.  To recognise you when you make use of the App.  We may use tracking information as described above in aggregate form to improve the App and services offered on it by carrying out statistical analyses of users’ activities and by measuring user demographics and interest in specific areas of the App. We may also provide such aggregated statistical data to our partners, including for the purposes of helping advertisers reach the kind of audience they want to target via the App. None of the aggregated statistical information provided to such partners personally identifies individual users of the App.  **COOKIES**  If patients like to manage use of cookies or completely turn off cookies, then they can do so by amending cookie settings in the internet browser.  Please note that if the patient does limit or block cookie use on our Site then the functionality of both the Site and our services may be affected.  The patient is asked to consider if they want a digital log of the visit to our Site to be recorded in their browser. If they don’t want a record to be kept, they can choose to delete browser history afterwards or view our pages in incognito mode / private browsing, which won’t store browser history, cookies, or search history after they closed your browsers. Using incognito mode / private browsing does not hide browser history from the internet service provider, us or their employer (if you are using a company device).  They can set your browser to refuse all or some browser cookies, or to alert when websites set or access cookies. If they disable or refuse cookies, please note that some parts of this Site may become inaccessible or not function properly.  Our Site uses cookies to distinguish patients from other users of our Site. This helps us to provide them with a good experience when they browse our Site and also allows us to improve our Site. By continuing to browse the Site, they are agreeing and give consent to our use of cookies.  A cookie is a small file of letters and numbers that we store on the browser or the hard drive of the computer if the user agrees. Cookies contain information that is transferred to the computer’s hard drive.  We use the following cookies:   * **Strictly necessary cookies.** These are cookies that are required for the operation of our Site. They include, for example, cookies that enable log into secure areas of our Site, use an online service or make use of e-billing services. * **Analytical/performance cookies.** They allow us to recognise and count the number of visitors and to see how visitors move around our Site when they are using it. This helps us to improve the way our Site works, for example, by ensuring that users are finding what they are looking for easily. * **Functionality cookies.** These are used to recognise users when you return to our Site. This enables us to personalise our content for them, greet them by name and remember their preferences (for example, choice of language or region). * **Targeting cookies.** These cookies record visits to our Site, the pages visited and the links followed. We will use this information to make our Site and the advertising displayed on it more relevant to their interests. We may also share this information with third parties for this purpose.   You can find more information about the individual cookies we use and the purposes for which we use them in the table below:   |  |  |  |  | | --- | --- | --- | --- | | **Cookie** | **Name** | **Purpose** | **More information** | | Cloudflare | \_\_cfduid | Used by Cloudflare to identify trusted web traffic | 3rd party cookie | | Stripe | \_\_stripe\_mid  And \_\_stripe\_sid  And m  And nsr | These cookies are necessary for making credit card transactions on the Site. The service is provided by Stripe.com which which allows online credit card transactions without storing card information. | 3rd party cookie | | Twitter | local\_storage\_support\_test | This cookie is used in context with the local storage function in the browser. This function allows the Site to load faster by pre-loading certain procedures | 3rd party cookie | | Google Analytics | \_ga,\_gid,  collect | Used to distinguish users. | First Party Cookie | | GoogleTag Manager | \_gat | Used for Google Tag Manager. | First Party Cookie | |  | loglevel | Used to make the Site’s video content more relevant to the visitor |  | | Twitter | \_widgetsettings |  |  | | You Tube | GPS, PREF, VISITOR\_INFO1\_LIVE, YSC, yt-remote-cast-installed, yt-remote-connected -devices, yt-remote-device-id, yt-remote-fast-check-period, yt-remote-session-app, ytr-remote-session-name | Used to store user preferences / other unidentified purposes | 3rd Party Cookie | | Doubleclick | IDE, test\_cookie | Used to distinguish users. | 3rd Party Cookie | | Linkedin | lidc | Used for tracking use of embedded services | 3rd Party Cookie | | Google | NID | Used to register a unique ID that identifies a returning user’s device | 3rd Party Cookie | | Infusionsoft | various | Used to associate a unique ID to other relevant information | 3rd Party Cookie | | Squeezy | PHPSESSID | Preserves user session state across page requests. | 1st Party Cookie |     Please note that third parties (including, for example, advertising networks and providers of external services like web traffic analysis services) may also use cookies, over which we have no control. These cookies are likely to be analytical/performance cookies or targeting cookies.  Except for essential cookies, all cookies will expire after variable times from a single session to 1 day through to 10 years. All cookies are annonymised. |
| 1. Please tick the data items that are held in the system     Personal  Special  category | Name  Address  Post Code  Date of Birth  GP  Consultant  Hospital/L A No.  Next of Kin  Sex  ID/NHS Number  Occupation  Local reference number  National Insurance Number  Contact details  Political opinion  Sexual orientation/life  Trade union  Religious/Philisophical  Genetic / biometric  Racial / Ethnic Origin  Health data  Treatment dates/Diagnosis  Criminal offences  Other (please state here): |
| 1. Will the asset collect new personal data items which have not been collected before? | Yes  No  Provide details below: |
| 1. What checks have been made regarding the adequacy, proportionality, relevance and necessity for the collection of personal and/or sensitive (special categories) of data for this asset? | Pseudonymisation  Anonymisation  Caldicott checks  Provide details below:  The LW PIA has been reviewed internally and a legitimate purpose for the data use has been identified. |
| 1. Is the third party contractor/supplier of the system registered with the Information Commissioner? What is their notification number? Please complete [Appendix 1 – Checklist for Third Parties](#_Appendix_1_–) | Yes  No  Not applicable  Company name and Data Protection ICO Number:  ZA347108 Living With |
| 1. Who provides the information for the asset? E.g. source of data (ref Information Asset Register IAR/Record of Processing ROP) | Patient  Staff  Others – Please specify  e.g. 3rd party, system, supplier, partner organisation |
| 1. What is the lawful basis for processing Personal Data under General Data Protection Regulation. DPA 2018   (Appendix 2 [click](#_Appendix_2_–))  (ref IAR/ROP)  NB –DO NOT select 6) (1) a) if processing is for the purpose of direct health or social care | |  | | --- | | 6) (1) a) Consent - (all article 7 conditions must be met | | 6) (1) b) Delivery of a Contract | | 6) (1) c) Legal Obligation | | 6) (1) d) Vital interests | | 6) (1) e) A public / official function / Interest | |  | |
| 1. Does the processing involve special categories of data (ref Question 4)? | Yes  No |
| 1. If Yes What is the lawful basis for processing Personal Data under General Datra Protection Regulation Article 9.   (Appendix 2 [click](#_Appendix_2_–))  NB –DO NOT select 6) (1) a) if processing is for the purpose of direct health or social care | |  | | --- | | 9) (2) a) Consent – (all article 7 conditions must be met) | | 9) (2) b) Employment, social security etc. | | 9) (2) c) Vital interests | | 9) (2) d) Legitimate activities (not to be used for public authorities) | | 9) (2) e) Data already been made public by subject | | 9) (2) f) Legal obligation | | 9) (2) g) Public interest | | 9) (2) h) Provision of Health or Social Care | | 9) (2) i) Public health | | 9) (2) j) Historical or scientific research | |  | |
| 1. Where consent is applied, Please provide details of the consent process and embed any consent forms   Note: Consent must follow Article 7 requirements ([Appendix 2 – Click](#_Appendix_2_–)) | Explicit consent  Provide details below: |
| 1. Please indicate other legislation which provides a legal basis for processing (Please tick relevant legislation or add details as necessary) | Children Act 1989 as amended 2004  Mental Capacity Act 2005  Health & Social Care Act 2012  Care Act 2014  H&SC (Safe and Quality) Act 2015  NHS Act 2006  Human rights Act 1998  Data Protection Act 2018 Sch 1 para 2  Other (Please specify) |
| 1. If relying on a contract for processing does the third party/supplier contracts contain all the necessary Data Protection clauses including information about Freedom of Information?   (check contract states GDPR/DPA2018) (Ref: Q7) | Yes  No  Provide details below:  Supplier DSP toolkit registered and GDPR compliance checked by external auditor |
| 1. Where the Data is being processed, detail where this is recorded / registered. | Information asset register / Record of Processing  Caldicott Approval  State where the information above is stored (ref No.of IAR/RoP and the asset number)  Contained in Annex to IG Manual |
| 1. How will the data be kept up to date and checked for accuracy and completeness? | Provide details below:  Validation in application plus prompts by application on patient timeline |
| 1. Who will have access to/share the information? Ref IAR/ROP   (Refer to your stakeholders and relationships lists in [Section](#_Section_A:_New/Change) A ) | Include any external organisations. Also how the data will be sent/accessed and secured.  Provide details below:  None |
| 1. Do you intend sending 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  If yes, have you obtained consent?  Provide details below: |
| 1. If answered Yes to Q18 – Does the asset comply with privacy laws such as the Privacy and Electronic Communications Regulations 2003 (Appendix 2 [click](#_Appendix_2_–)) | Yes  No  Not applicable  If yes provide details below: |
| 1. 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 |
| 1. 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 |
| 1. Is there a useable audit trail in place for the asset? For example to identify who has accessed a record. | Yes  No  If no flag to DSP team. |
| 1. Can the data be easily obtained by the data Subject upon request? | Yes  No |
| 1. Have you assessed that the processing of personal / special categories of data will not cause any unwarranted harm to the rights and freedoms of the individuals concerned?   What risk assessment has been carried out?  ([Appendix 3 click](#_Appendix_3_–) ) | Yes  No  Embed risk assessment if separate document  DPIA review conducted each time an implementation occurs |
| 1. Do you have a compliant Privacy Notice | Yes  No  If yes Embed here  An updated privacy policy is attached to this document |
| 1. What are the retention periods for this data? (please refer to the NHS Code of Practice Records Management ) | We comply with the NHS code of practise for data retention. |
| 1. How will the data be destroyed when it is no longer required? | Provide details below:  Removal from database, data backups and data archives using active overwrite tool |
| 1. Does the asset involve new linkage of personal data with data in other collections, or are there significant changes in data linkages? | Yes  No  If yes provide details below: |
| 1. Where will the data be kept/stored/accessed? | On paper  On a database saved on a network folder/drive  external Website / system  On a dedicated system saved to NHS network  Other – please state below: |
| 1. Will any data be transferred outside the organisation premises or systems?   If ‘Yes’ where is this information being sent | Yes  No  Please provide details:  The patient may choose to share their information when visiting their GP |
| 1. Please state by which method the data will be transported. | non secure Email  Secure Mail  Website  courier  By hand  post – internal  telephone  post – external  Secure File Transfer Other – please state below:  Health care professionals with a legitimate interest may access the patient record directly in the app. The patient may choose to share their information with their GP by hand (printed copy) during a consultation. There is no data sharing feature in the app. |
| 1. What level of encryption is being used where transfer is electronic? | Please provide details:  Not transferred |
| 1. Are you transferring any personal and / or sensitive data to a country outside of the UK?   Please name the country  Does this include back-up arrangements? | Yes –Within the European Economic Area (EEA)  Yes –Outside the European Economic Area (international)  No  Provide details below |
| 1. If transfer is outside of the EEA, what measures are in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country?   (DPO to assess ICO decision for bulk transfers) | Please provide details:  None |
| 1. All transfers outside of the UK must be approved by the organisation Data Protection Officer (DPO)   Please provide DPO documented approval | Please provide details:  None |
| 1. Is there a Security Management Policy and Access Policy in place? Please state policy titles. | Yes  No  NHS DSP toolkit compliant IG Manual |
| 1. Is the Processor compliant with the 10 data and cyber security standards – the ‘17/18 Data Security Protection Requirements’ (2017/18 DSPR) | ISO/IEC 27001:2013 (Not certified)  Cyber Essentials Plus (CE+) certification  Digital Marketplace  Other (please state) NHS DSP Toolkit compliant  Evidence provided:  Yes  No Externally audited |
| 1. Has an information risk assessment been carried out and reported to the Information Asset Owner (IAO)?   (Ref. IAR / RoP) | Yes  No  Please provide details below as to how the risks will be managed and mitigated (include any inclusion of relevant risk register)  See risk register, signed off by SIRO/IAO |
| 1. Is there a contingency plan / backup policy in place to manage the effect of an unforeseen event? Please provide a copy. | Yes  No  See IG Manual |
| 1. 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  If yes provide details and procedure / policy titles below:  Data back up using AWS |

## Section C - Sign off, actions and outcomes

**\*\*\*\*\*Data Security and Protection To Complete\*\*\*\*\***

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **DPIA Reviewed by** |  | | | | **Review Date** | | | |  |
| **IT Servicedesk Reference** |  | | | | **DPIA Central Register Reference** | | | |  |
| **Summary of DSP Advice:** | | | | | | | | | |
| **Action Asigned** | | | **Responsibility** | | | **Due** | | **Completed** | |
|  | | |  | | |  | |  | |
| **Risk Mitigations approved by:**  ***(a person of seniority on the project)***  Integrate actions back into project plan, with date and responsibility for completion. | | | Click here to enter text. | | |  | | Click here to enter text. | |
| **Remaining Risks accepted by:**  ***(a person of seniority on the project)***  If any risks remain that cannot be mitigated or reduced please detail | | | Click here to enter text. | | |  | | Click here to enter text. | |
| Can the DPIA be passed to Data Protection Officer for Approval?  If no please state reason why and return form to lead who completed it. | | | Yes  No | | |  | |  | |
| **DPO Advice Provided** 🞎YES | | | | | | **Date** | |  | |
| **Summary of DPO advice:** | | | | | | | | | |
| **DPO advice accepted** 🞎YES 🞎NO ***NB: If no state reason why below*** | | | | | | | | | |
| **Comments:** | | | | | | | | | |
| **Residual High risk** 🞎YES 🞎NO ***(if yes report to ICO)*** | | | | | | | | | |
| **ICO Outcome:** | | | | | | | | | |
| **DPIA Approved** 🞎YES - IT Servicedesk Reference 🞎NO  DATE:  If no please justify | | | | | | | | | |
| **DPIA Review Due Date** | |  | | **DPIA Owner** | | |  | | |

**NB- Under Current Data Protection legislation DPIAs must be approved by organsiations Data Protection Officer (DPO)**

## Appendix 1 – Checklist for Third Parties

|  |  |
| --- | --- |
| **Third Party Details:** | |
| **Third Party Name:** |  |
| **Address:** |  |
| **Contact No.** |  |
| **Name of Key contact:** |  |
| **Contact details of key contact:** |  |
| **Data Protection Notification No.**  ***(if registered with the ICO)*** |  |
| **Please describe the service that is being supplied:** |  |

|  |  |  |
| --- | --- | --- |
| **Data Protection Checklist:** | | |
| **1** | **What data are you processing on our behalf?** | Patient medical data |
| **2** | **Where will you be processing the data? Detail sites** | Amazon Web Service |
| **3** | **Will your staff have remote access to the NHS/LA data? If so, please explain.** | N |
| **4** | **Will you be storing any NHS/LA data in hard copy for any length of time? *If so, how will the data be stored?*** | N |
| **5** | **Will you be storing any NHS/LA data in electronic format?**  ***If ‘Yes’ complete 5a – 5h)*** | Y |
| **6** | **Is the data encrypted at rest? If so to what standard?** |  |
| **7** | **Do all users of your systems have their own log-in and password?** | Y |
| **8** | **What is your password policy for accounts that can access NHS/LA data?** | Our own password policy set down in IG Manual |
| **9** | **Do you have a password rotation policy? If so how often are the passwords changed?** | Y – every 3m |
| **10** | **How are access rights to systems controlled / managed?** | Role based access control RBAC on log in |
| **11** | **Are back–ups containing NHS/LA data encrypted? If so to what standard?** | Y |
| **12** | **What protection do you have against malicious code?** | Antivirus protection |
| **13** | **How often do you apply security patches?** | Automatically |
| **14** | **How often do you risk assess your security controls?** | Monthly |
| **15** | **What business continuity/disaster recovery plans do you have in place?** | See IG manual – plus AWS have extensive DR plans |
| **16** | **Are USB ports/CD writers on staff equipment disabled?** | Y |
| **17** | **If not explain what measures are taken to ensure NHS/LA data is not exported to removable media without permission.** | N/a |
| **18** | **Will you be storing data outside the UK? *If so, where? What information governance considerations have been taken into account?*** | N |
| **19** | **Will the data be linked with any other data collections? *If so, how will the link be achieved?*** | N |
| **20** | **What security controls do you have in place for your office premises?** | Physical security measures include locks, alarms, visitors register, remote monitoring by security company |
| **21** | **What controls do you have in place for the security of your equipment?** | Password protection, locked away when not in use, remote erasing enabled |
| **22** | **Have you had any security incidents relating to data in the last three years? *If so, please provide details.*** | None |
| **23** | **What policies do you have in relation to information security, data protection and incident reporting? *Please provide copies.*** | See IG manual |
| **24** | **Describe potential disciplinary actions for breach of policy.** | Various depending on severity up to nd including dismissal |
| **25** | **How do you ensure the people your recruit have the honesty and integrity to handle personal data?** | HMG BPSS security standard compliant |
| **26** | **How do you ensure your staff understand the importance of data security and how to keep personal data secure?** | Induction and annual awareness sessions |
| **27** | **How frequently do you provide your staff with training on data security / confidentiality and is their learning tested?** | Annual |
| **28** | **Will you ever transfer NHS/LA data electronically? *If so, how?*** | N |
| **29** | **If yes will the data be encrypted In transit, if so to what standard?** | N/A |
| **30** | **Will you transport any NHS/LA hard copy data? *If so, what security controls will be in place?*** | N |
| **31** | **Will you ever destroy any NHS/LA data?**  ***If so, what method is used and what evidence of destruction will be provided?*** | Y  Active overwrite package used and certificate provided |
| **32** | **Will you ever sub-contract work in relation to NHS/LA data?**  ***If so, in what circumstances?*** | N |
| **33** | What is the source of the data | See attached data flow |
| **34** | How the data will be collected, used, stored and deleted | Covered on data flow |
| **35** | What processing may be considered high risk | None |
| **36** | How often is data collected? | Daily as per treatment plan for patient |
| **37** | How many people does the processing affect? | 1000’s of patients |
| **38** | What geographical area is covered? | England, Wales, Scotland and Northern Ireland. |
| **39** | Is the processing novel in any way? | No |
| **40** | Confirmation of all lawful basis for processing | Contract requirement  Healthcare treatment |
| **41** | Would individuals reasonably expect their data to be processed in this way? If not, can you justify the unexpected processing? | Yes patients aree familiar with GPs using electronic patient record systems |
| **42** | How might the processing affect individuals and can you can justify any adverse impact | Processing improves patient experience  No adverse impact |
| **43** | How did you obtain the data? Can you evidence you did this fairly (without misleading/deceiving individuals?) | Yes collected fairly.  Data flow shows evidence of consent |
| **44** | What steps have you taken to inform individuals about the ways in which the Developer is processing individuals personal data | This is explained to patients before they are signed up by their clinicians – patients have to be invited to use the app and service, they cannot simply access the service by downloading from the app store. The EULA provided to patients during the sign up process also defines how personal data is used. |
| **45** | Identify the Rights of individuals based on the lawful basis for  processing. How will individual be made aware of their rights and what are they? | Set out in privacy policy publicised on web site |
| **Date completed:** | | 14/7/2020 |
| **Completed by:** | | Ian Harrison |
| **Telephone number and email address:** | | via email to David Anahory |
| FOR IT Use Only | | |
| **Appendix 1 Reviewed by** | |  |
| **Review Date** | |  |
| **IT Servicedesk Reference:** | |  |
| **Summary of IT Security Advice / Findings:** | |  |
| **Appendix 1 approved** | | Yes  No |
| **If No actions to be completed by lead** | |  |

# Appendix 2 – Glossary of Terms

|  |  |
| --- | --- |
| Item | Definition |
| 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:   1. from those data, or 2. 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:   1. racial or ethnic orign of the individual 2. the political opinions of the individual 3. the religious or philosophical beliefs of the individual 4. whether the individual is a member of a trade union 5. processing of genetic or biometric data for uniquely identifying an individual 6. physical or mental health of the individual 7. sex life or sexual orientation of the individual |
| **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. |
| **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 casenotes) 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 very 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 (GDPR)** | European legislation (applied in UK law by the Data Protection Act 2018) on the protection of natural persons with regard to 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, jept 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 dta 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. |
| **Article 6 Conditions of Processing** | 1) (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes -  only lawful if ALL article 7 conditions for consent are met  1) (b) A contract with the individual: for example, to supply goods or services they have requested, or to fulfil your obligations under an employment contract. This also includes steps taken at their request before entering into a contract.  1) (c) Compliance with a legal obligation: if you are required by UK or EU law to process the data for a particular purpose, you can.  1) (d) Vital interests: you can process personal data if it’s necessary to protect someone’s life. This could be the life of the data subject or someone else.  1) (e) A public task: if you need to process personal data to carry out your official functions or a task in the public interest – and you have a legal basis for the processing under UK law – you can. If you are a UK public authority, our view is that this is likely to give you a lawful basis for many if not all of your activities.  1) (f) Legitimate Interest: If you need to process personal data in the legitimate interests of the Data Controller or 3rd Party or Data Subjects Rights in particular where data subject is a child.  NB 1) (f) does not apply to processing carried out by Public authorities in the performance of their tasks. |
| **Article 9 Conditions of Processing special categories of data** | (1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.  (2) Paragraph 1 shall not apply if one of the following applies:  2) (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject  only lawful if ALL article 7 conditions for consent are met (see column D)"  2) (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;  2) (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;  2) (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;  2) (e) processing relates to personal data which are manifestly made public by the data subject;  2) (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;  2) (g) processing is necessary for reasons of substantial public interest, on the basis of 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;  2) (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;  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 quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;  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. |
| **Article 7 (Recital 32) Conditions for Consent** | Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject’s acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject’s consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided. |

# Appendix 3 – Examples of Risk

|  |
| --- |
| **EXAMPLES OF PRIVACY AND RELATED RISKS** |
| **RISKS TO INDIVIDUALS** |
| Inadequate disclosure controls increase the likihood of information being shared inappropriately. |
| The context in which information is used or disclosed can change over time, leading to it being used for different purposes without peoples knowledge. |
| New surveillance methods may be an injustified intrusion on their privacy. |
| Measures taken against individuals as a result of collecting information about them might be seen as intrusive. |
| The sharing and merging of datasets can allow organisations to collect a much wider set of information that individuals may expect. |
| Identifiers might be collected and linked which prevent people from using a service anonymously. |
| Vulnerable people may be particularly concerned about the risks of identification of the disclosure of information. |
| Collecting information and linking identifiers may mean that an orgainsation is no longer using information which is safely anonymised. |
| Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk. |
| If a retention period is not established information might be used for longer than is necessary. |
| **CORPORATE RISKS** |
| Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage. |
| Problems which are only identified after the project has launched are more likely to require expensive fines. |
| The use of biometric information or potentially intrusdive tracking technologies may cause increased concern and cause people toaviod engagement with the organisation. |
| Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business. |
| Public distrust about how information is used can damage an organisations reputation and lead to loss of business. |
| Data losses which damage individuals could lead to claims for compensation. |
| **COMPLIANCE RISKS** |
| Non-compliance with the DPA. |
| Non-compliance with the Privacy and Electronic Communications Regulations (PECR) |
| Non-compliance with sector specific legislation or standards |
| Non-compliance with Human Rights legislation |