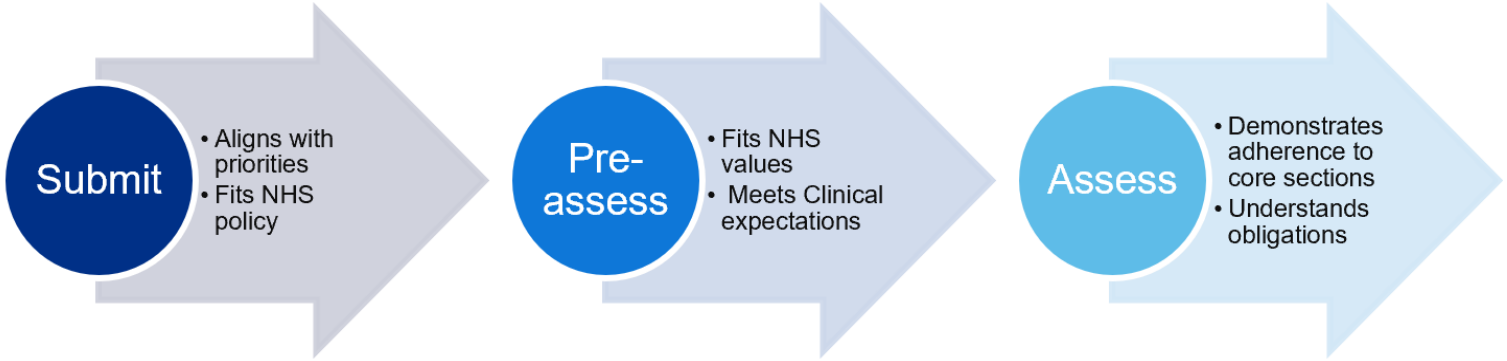
Digital Assessment Questionnaire V2.1

This is an indication of the NHS digital assessment for the use of mobile apps and other patient-facing digital tools. This is currently used to assess mobile apps and digital tools for inclusion in the NHS Apps Library.
Manufacturers/Developers of Digital Technologies for use in the NHS should review the document to better understand the required standards expected to be showcased across other NHS tools, including the NHS Apps Library. This represents a full list of all possible questions. **Not all questions will be relevant to all developers. The online assessment will apply the relevant questions.**

Any questions or comments relating to this document can be sent to m.health@nhs.net or if you would like to apply become an approved assessor against these questions, you can email m.health@nhs.net with the subject title "Approved Assessor enquiry".

Last update 16/08/18



Pre-assessment - Stage 1

Establishing suitability for the App or digital tool to be invited in for full assessment.

Question	Response	Relevant Guidance
Name of company and brief description		
Please can you give the registered address of your company.		
Key contact individual Name, email and contact number		
Is your product available to the public?	Yes|No	
Does your product use any form of NHS Branding?	Yes|No	https://www.england.nhs.uk/nhsidentity/faq/can-we-use-the-nhs-letters-in-our-company-name/
Have you reviewed the Eligibility Questions and Digital Assessment Questions? https://developer.nhs.uk/digital-tools/daq/	Yes and we can respond to all applicable questions | Yes but we cannot respond to all applicable questions, we are working towards that. | No	
Do you or your organisation carry on or propose to carry on any regulated activities in England which require registration with the Care Quality Commission (CQC)?	Yes|No	These are laid out in Schedule 1 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014.
If 'yes', Are you registered with CQC?	Yes|No	
If 'yes', Please provide your CQC Account Number, and the date of your most recent registration certificate, the date and outcome of your last CQC inspection. If you have not been inspected, please can you provide a date of you upcoming inspection.		
If 'yes', Have you reviewed the Scope of Registration for CQC, and confirmed your activities do not require registration.	Yes, I have reviewed and confirmed our activities do not require registration |No, I have either not reviewed, or not confirmed our activities do not require registration.	Please note carrying on Regulated Activities in England without registration is a criminal offence.

Please confirm that you will keep your activities under review: changes to the activities which you perform as part of your service may bring it into scope of registration with CQC, require the registration for additional regulated activities, or the scope of registration may change over time bringing with it a new requirement to register.	Yes, I confirm we will keep our activities under review| No, we will not keep our activities under review.	Please note carrying on Regulated Activities in England without registration is a criminal offence.
Is your product free to the public?	Yes|No	
If 'no', How much does the app costs (please include 'in-app' costs)?		
If 'no', What is the source of the funding		
If 'no', Currency: Charge £ /		
Can you describe your business model. Please include any direct costs e.g. licence cost, purchase cost, subscription for use,		

Pre-assessment - Stage 2

Establishing if you meet the current eligibility for the App or digital tool to be invited in for full assessment.

Note: Eligibility criteria is based on the current priorities within the NHS and may change to reflect changing priorities

Question	Response	Relevant Guidance
Please briefly describe your product?		
In what situations/context to you envision it to be used?		
Who is/are the intended end-users?		
What problem in the health system or to the end-user is your product trying to solve?		
Estimate the population who would use the product (per 100,000 population)		
Do you think your product could replace a current NHS commissioned service?	Yes|No	
If 'yes', What type commissioned service would it replace?		
Does your product require registration or login details for full use of the product?	Yes|No	
If 'yes', Please provide guest login		
Does the tool integrate with a website or other software/device?	Yes|No	
If 'yes', Please describe all applicable functionality		
Does the product intend to connect to any of the following services? Select all that apply		
a. Health and Social Care Network	Yes|No	
b. NHS Mail	Yes|No	
c. Spine	Yes|No	
d. Summary Care Records	Yes|No	
e. NHS Pathways	Yes|No	
f. Electronic Referrals Service (eRS)	Yes|No	
g. Electronic Transfer of Prescription Service (ETP)	Yes|No	
h. GP2GP	Yes|No	
i. GP Connect	Yes|No	

j. GPSoC Connection to Primary Care Systems (EMIS, TPP, VISION & Microtest)	Yes|No	
k. Other		
Please select the statements that apply to your product Select **all** that apply		
It is a clinical decision support system. It contributes to decisions about treatment and may involve controlling other medical devices	Yes|No	
It is used as a calculator which provides information which impact treatment, diagnosis or care. This information is obtained by analysing data entered by the user or collected by the device	Yes|No	
It is used to provide a psychological intervention to people with a diagnosed condition	Yes|No	
It is used to facilitate the diagnosis or management of a condition by collecting information. It may include features such as reminders or alerts	Yes|No	
It is used to facilitate communication with professionals	Yes|No	
It is used to promote behaviour change to reduce personal risk factors for a specific condition	Yes|No	
It enables people to interact with their data or appointments in the NHS or social care systems	Yes|No	
It enables people to communicate with others	Yes|No	
It collects information to enable people to keep a personal record. This data is not routinely shared	Yes|No	
It provides information to promote learning and improve awareness	Yes|No	
It provides a digital solution to businesses (e.g. appointment booking or staff rotas)	Yes|No	
It is used as an information or service finder and holds no personal data	Yes|No	
It is used as an eBook or digital book equivalent	Yes|No	
Which platforms and versions of the product are available?		
a. iOS	Yes|No	
If 'yes', please specify the version number	Yes|No|Not applicable	
b. Android	Yes|No	
If 'yes', please specify the version number	Yes|No|Not applicable	
c. Windows Mobile	Yes|No	
If 'yes', please specify the version number	Yes|No|Not applicable	
d. OS X	Yes|No	
If 'yes', please specify the version number	Yes|No|Not applicable	
e. Linux	Yes|No	
If 'yes', please specify the version number	Yes|No|Not applicable	

f. Other		
Does your product process (e.g. store) personal data of NHS or Social Care patient/client/service users?	Yes|No	
If 'yes', where does the product process and store personal data of NHS or Social Care patient/client/service users?		
If 'other' please tell us where?		
Please tell us the health condition(s) or theme(s) that your product is aimed at?		
Are you involved in a pilot / trial with a NHS hospital, trust, Clinical Commissioning Group (CCG) or primary care setting?		
Please give brief details and a contact name of a CCG referee		
Please list the functionality of the app - Include any calculating functions (e.g. Body Mass index, Weights charts for children, calorific counters) and any associated information outputs e.g. dietary or exercise suggestions.		
Please describe if and how the digital service integrates with other systems (e.g. a GP System or a parent System. Other examples may include patient administration or prescribing systems.)		
Is your digital tool a medical device as defined within the Medical Device Directive? Please check the guidance provided by MHRA.	Yes|No	https://www.gov.uk/government/publications/medical-devices-software-applications-apps
If 'Yes', Please provide evidence confirming agreement from MHRA or a notified body.		
if don't know , does the digital tool indicate a diagnosis, treatment, is used for monitoring of a physiological process or disease, supports clinical decisions, performs calculations or indicates individual risk scores for a medical purpose?	Yes|No	If the answer is 'Yes' to any of the listed uses, then the digital tool probably falls under the category of a medical device and guidance must be sought from the MHRA. On line guidance should be consulted first, this includes guidance on device classification: https://www.gov.uk/government/publications/medical-devices-software-applications-apps Specific regulatory questions should be addressed to Devices.Regulatory@mhra.gsi.gov.uk

If defined as a medical device the digital tool should be is 'CE' marked to show the manufacturer's declaration that the application complies with the EU Medical device directives. Please provide the following evidence: Class 1 devices [most] - evidence of registration with MHRA and self-declaration of conformity, or Class 11a and above devices - CE certificate from a Notified Body All - Your post market surveillance plan.	Yes|No	Please upload evidence
Does your digital tool constitute a pharmacy service that requires registration with the General Pharmaceutical Council?	Yes|No	
Does your digital tool form part of a service that requires registered health or care professionals to operate?	Yes|No	
Please confirm registration status and fitness to practice in England by suppyling names of registrants and appropriate identifiers/codes.		This only applies where you manage the digital tool and the health or care staff.

Assessment stage - Effectiveness

Establishing if you have appropriate evidence to demonstrate improved outcomes.

Question	Response	Relevant Guidance
Are there any clinical benefits to using your product?	Yes|No	
If 'yes', please describe what, when, timeframe for improved outcomes		
Do you have any evidence to show success of the clinical benefits? e.g published articles, pilot studies in place, user research?	Yes|No	https://www.cebm.net/2009/06/oxford-centre-evidence-based-medicine-levels-evidence-march-2009/
If 'yes', please select relevant evidence type(s)	• Expert opinion without explicit critical appraisal, or based on physiology, bench research or "first principles" • Case series (and poor-quality cohort and case-control studies) • Individual case-control study • Systematic review (with homogeneity) of case-control studies • "Outcomes" Research; ecological studies • Individual cohort study or low quality randomized controlled trials (e.g. <80% follow-up) • Systematic reviews (with homogeneity) of cohort studies • All or none randomized controlled trials • Individual randomized controlled trials (with narrow confidence interval) • Systematic reviews (with homogeneity) of randomized controlled trials	
If 'yes' please upload document(s) or relevant url(s) of evidence		
If No, please give reason why?		
Are there any *behavioural* benefits to using your product? For e.g will it improve patient reported outcomes or experience measures?	Yes|No	
If 'yes', please describe the improvements to psychological or social motivation/ PROM/PREMs		

Do you have any evidence to show success of the behavioural benefits? e.g published articles, pilot studies in place, user research	Yes|No	https://www.cebm.net/2009/06/oxford-centre-evidence-based-medicine-levels-evidence-march-2009/
if 'yes', indicate which of the below and upload document or add hyperlink	• Expert opinion without explicit critical appraisal, or based on physiology, bench research or "first principles" • Case series (and poor-quality cohort and case-control studies) • Individual case-control study • Systematic review (with homogeneity) of case-control studies • "Outcomes" Research; ecological studies • Individual cohort study or low quality randomized controlled trials (e.g. <80% follow-up) • Systematic reviews (with homogeneity) of cohort studies • All or none randomized controlled trials • Individual randomized controlled trials (with narrow confidence interval) • Systematic reviews (with homogeneity) of randomized controlled trials	https://www.cebm.net/2009/06/oxford-centre-evidence-based-medicine-levels-evidence-march-2009/
If 'yes' please upload document(s) or relevant url(s) of evidence		
If 'no', please give reason why?		
If there are no specific clinical or behavioural benefits, what other outcomes have you measured?		
Has your product been evaluated at all for these other outcomes?	Yes|No	

If 'yes', indicate which of the below and upload document or add hyperlink (upload document link)	• Expert opinion without explicit critical appraisal, or based on physiology, bench research or "first principles" • Case series (and poor-quality cohort and case-control studies) • Individual case-control study • Systematic review (with homogeneity) of case-control studies • "Outcomes" Research; ecological studies • Individual cohort study or low quality randomized controlled trials (e.g. <80% follow-up) • Systematic reviews (with homogeneity) of cohort studies • All or none randomized controlled trials • Individual randomized controlled trials (with narrow confidence interval) • Systematic reviews (with homogeneity) of randomized controlled trials	
If 'yes' please upload document(s) or relevant url(s) of evidence		
If No, please give reason why?		
Are there are any resource costs associated with running the service, or any activities assumed to be undertaken by health or care staff. I.e are there any indirect costs of facilitating use, e.g. time required for remote monitoring. If directly replacing a process, please provide details of the resources needed here, and the comparative service costs being replaced		
Based on your business model and costs, are there resource impact benefits associated with your product?		
Is there cost and resource impact data available to demonstrate the claimed economic benefits of your product?		

Assessment stage - Clinical Safety

Establishing if you have appropriate safety measures and safeguards.

Question	Response	Relevant Guidance
Does the digital service fall within the scope of the NHS England mandated Safety Standard (DCB0129).	Yes|No	https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0129-clinical-risk-management-its-application-in-the-manufacture-of-health-it-systems
Which functionality and areas of scope have you deemed applicable and provide a copy of your Safety Case and Hazard Log.		Safety Case and Hazard Log template can be found at - https://digital.nhs.uk/services/solution-assurance/the-clinical-safety-team/clinical-safety-documentation
Please provide a brief explanation as to why it does not fall within the scope of the NHS England mandated Safety Standard (DCB0129).		
Is it possible for users to experience adverse effects as a result of using the digital service	Yes|No	E.g. think about what may happen if the information displayed within the app is missing, incorrect or displayed in a confusing manner, could this have an effect on the user or the care/treatment they receive?
Please list all of the possible adverse effects		
Please list any adverse events associated with the digital service reported to a notified body, regulatory authority or known to you from other sources?		
Has the safety assessment for the digital service and its impact on interfacing systems been reviewed and approved by a suitably qualified clinician or other Health Care Professional?	Yes|No	
Please provide name and job title.		

Assessment stage 1 - Data Protection - Processing (all)

This section is to be completed by all applicants. This section aims to identify the type of data being, or intended to be, processed (to determine whether Data Protection laws apply).

.

Category	Question	Response	Relevant Guidance
Personal Data	Is any of the following **personal data** intended to be processed (e.g. collected /used) using the digital tool/app? Also consider and include access your tool /product may gain to other existing personal data e.g. mobile phone photo library.		Two examples to help differentiate between personal and sensitive personal (health) data: · An app allows a user to track whether he has taken her prescribed medications and thus complies with the advice provided by a doctor. This app processes data concerning health, since the consumption of medication is indicative of the health of an individual. · An app tracks footsteps solely as a way of measuring the users' sports activities during a single walk. The data is not stored by the app developer to create a profile that evaluates the user's physical fitness or health condition, nor is it combined with other data. This app does not process data concerning health - so it is not Sensitive Personal Data, however, it is still Personal Data about the lifestyle of the individual. However, if the data is also used to measure or predict health risks (e.g. risk to injury or heart attacks) and/or stored in order to analyse and evaluate the user's health, then the app does process data concerning health (Sensitive Personal Data). **Data protection law applies whenever any type of personal data OR sensitive personal data is processed.**
Personal Data	Name|Address|Postcode (full)| Email Address|Home Phone Number|Mobile Phone Number / Device Number |DOB| Age|Sex (observed)|Gender (self declared)|Marital Status|Living Habits |Physical Description|General Identifier e.g. NHS No|Income / Financial / Tax Situation|Education / Qualifications|Employment / Career History|Professional Training / Awards|Cookies, web beacons, flash cookies, server logs etc which track individual's browsing behaviour | Other online identifiers e.g. IP address (static and dynamic) / Event Logs|Device IMEI No|Location Data (Travel / GPS / GSM Data / radio frequency identification tags (RFID))|Device MAC Address (Wireless Network Interface)	Yes|No|Not Sure	Personal Data: [Information relating to the individual] any information relating to an identified or identifiable (living) person. An identifiable person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
	Is any of the following **sensitive personal data** intended to be processed (e.g. collected /used) using the digital tool/app?? Also consider and include access your tool /product may gain to other existing personal data e.g. mobile phone photo library.		
Sensitive Personal Data	Physical / Mental Health or Condition (past, current or future status) including: · Medical data – data that are inherently/clearly medical data · Raw sensor data – data that can be used in itself or in combination with other data to draw a conclusion about the actual health status or health risk of a person · Conclusions data – data where conclusions are drawn about a person's health status or health risk, irrespective of whether these conclusions are accurate, or otherwise adequate |Family|Sexual Life / Orientation|Family / Lifestyle / Social Circumstance|Political opinion|Offences Committed / Alleged to have Committed / Criminal Proceedings / Outcomes / Sentence* |Financial data (that might be used for payment fraud)|Religion or Other Beliefs|Trade Union membership|Racial / Ethnic Origin|Biometric Data (e.g. fingerprints / facial Recognition) for the purpose of uniquely identifying a person|Genetic Data for the purpose of uniquely identifying a person	Yes|No|Not Sure	Sensitive Personal Data [Information relating to the individual] (also known as Special Categories of Personal Data): This is personal data (as defined earlier) but which is more sensitive and data protection legislation says it needs more protection. *Processing of criminal convictions data is prohibited unless carried out under the control of official authority

Personal & Sensitive Personal Data	If you have responded “Not sure” to any of the questions, please check the guidance on ICO's website (https://ico.org.uk/). Please confirm that you have visited ICO's website	Yes|No	
Personal & Sensitive Personal Data	If, after visiting the ICO website, you are still not sure then please describe the situation here and continue.		
Personal & Sensitive Personal Data	If you process additional personal data or sensitive personal data not listed above, can you please list them here?		
Personal & Sensitive Personal Data	If your response to one or more of the data items is “Yes” then personal data (either personal data or sensitive personal data) is being processed so please continue with the questionnaire. If your response to all ALL these data items is “No” then personal data (either personal data or sensitive personal data) is NOT being processed and you are not required to complete the remainder of the Data Protection Sections of the questionnaire.		**If all data categories in both Personal Data AND Sensitive Personal Data are all answered “No" – then the organisation is not processing personal data then data protection legislation will not apply to your tool, there is no need to continue answering other questions.**
Organisation Status	Who decides the purpose (and how) the personal data is processed? The next question will help identify if you/your organisation is a Controller or a Processor or neither i.e. a digital tool manufacturer only. The statement below covers only personal data processed by the digital tool – not other processing you may carry out e.g. employees’ personal data processed for employment purposes.		
Organisation Status	You/your organisation (does not need to actually possess the personal data) but STILL, alone or jointly with another organisation, decides: ⍰ to collect the personal data in the first place and the legal basis for doing so; ⍰ which items of personal data to collect, ie the content of the data; ⍰ the purpose or purposes the data are to be used for; ⍰ which individuals to collect data about; ⍰ whether to disclose the data, and if so, who to; ⍰ whether subject access and other individuals’ rights apply ie the application of exemptions; and ⍰ how long to retain the data or whether to make non-routine amendments to the data. **Notes:** **If your answer to these statements is "Yes", then your organisation is a "Controller" - please continue with the Data Protection Sections of the questionnaire** **If your answer to these statements is "No", then your organisation is a not a "Controller" - but please answer the remaining "Organisation Status" questions which follow.**	Yes|No|Not Sure	The ICO website has guidance for "key" terms including determining "Controller" status: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/
Organisation Status	You/your organisation processes personal data on behalf of another organisation(s) and the other organisation(s) makes the decisions which are described in 5a.7.1 **Note - If your answer to this is Yes, then you / your organisation is a "Processor".** Please do NOT complete the remainder of the Data Protection Sections of the questionnaire, contact us, letting us know the Controller" organisation, on whose behalf, you are processing personal data and submit your questionnaire with the partially completed Data Protection Sections.	Yes|No|Not Sure	‘Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.”

Organisation Status	You/your organisation is developing, or has developed, a digital tool/app, which will be used by a client to process personal data for which the client will be responsible (i.e. the client will be the "Controller" and make the decisions which are described in 5a.6.1 regarding the personal data processed by the client when using you tool/app. **Note - If your answer to this is Yes,then you / your organisation is a manufacturer or designer (neither a "Controller" nor "Processor"). You app must be designed and configurable to meet the potential clients' legal requirements.** Please see the Tooltip for more information and only complete Section 5c, which contains: •Data Protection Impact Assessment - Screening Questionnaire •Data Protection Impact Assessment Report – the content is sufficiently comprehensive to comply with legislation	Yes|No|Not Sure	If you are developing (manufacturing) a digital tool/app which you/your organisation then intends to make directly available to individuals i.e. citizens/the public, then the "Controller" accountabilities will fall to you/your organisation and you should complete all the data protection sections of the questionnaire. If, however, you are developing a digital tool/app, which will be used by another organisation such as a health or care organisation/professional to process personal data i.e. your potential client, who will be the "Controller of the personal data processed by the tool/app, then those clients will be accountable for evidencing compliance with relevant: •legislation (e.g. Data Protection legislation) •policies (e.g. "NHS and social care data: off-shoring and the use of public cloud services" https://www.digital.nhs.uk/article/8486/NHS-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services) and •regulations (e.g. "Medicines and Healthcare products Regulatory Agency" https://www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency). As part of your development process, you should ensure that you evidence that your digital tool/app, as a minimum, is designed to meet such requirements when it is taken into use by the client e.g. complies with two major principles required Data Protection Act 2018: •"Data Protection by design" which means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage •"Data Protection by default" which means that service settings must be automatically data protection friendly To evidence compliance with these principles you should complete the data protection questionnaire section (5c.) relating to: •Data Protection Impact Assessment - Screening Questionnaire •Data Protection Impact Assessment Report – the content is sufficiently comprehensive to comply with legislation
Processing Personal Data Outside the European Economic Area	You/your organisation is established in the EU and is therefore subject to EU and UK data protection legislation.	Yes|No|Not Sure	
Processing Personal Data Outside the European Economic Area	You/your organisation is based outside the EU and offers services to EU residents (for free or in return for payment).	Yes|No	
Processing Personal Data Outside the European Economic Area	You/your organisation is based outside the EU and monitors the behaviour of EU residents.	Yes|No	
Processing Personal Data Outside the European Economic Area	The personal data (or sensitive personal data) includes NHS or social care data	Yes|No|Not Sure|Not Relevant	
Processing Personal Data Outside the European Economic Area	If 'yes', you/your organisation complies with "NHS and social care data: off-shoring and the use of public cloud services" https://www.digital.nhs.uk/article/8486/NHS-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services	Yes|No|Not Sure|Not Relevant	
Processing Personal Data Outside the European Economic Area	If you have responded "Not sure" to any of the questions, please check the guidance on ICO's website (https://ico.org.uk/). Please confirm that you have visited ICO's website	Yes|No	

Processing Personal Data Outside the European Economic Area	If, after visiting the ICO website, you are still not sure then please describe the situation here, submit your questionnaire and request our guidance before continuing.		
The Data Protection Fee (Annual)	If 'yes', what is your registration number (in the Data Protection Register)?		In UK, Controllers must pay a data protection fee. This replaces the requirement to 'notify' (or register). The Data Protection (Charges and Information) Regulations 2018 requires every organisation that processes personal information to pay a fee to the Information Commissioner's Office (ICO). https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/
The Data Protection Fee (Annual)	If 'yes', but you do not have a registration number (in the Data Protection Register), explain why you do not have a registration number (in the Data Protection Register)		
ICO Data protection assurance	If 'yes', then complete the ICO Controller Checklist available at: https://ico.org.uk/for-		

Assessment stage 2 - Data Protection - DPIA

This section includes a screening questionnaire to identify whether a Data Protection Impact Assessment is required

Question	Response	Relevant Guidance
You/your organisation's intended processing involves systematic monitoring such as monitoring of wellness, fitness and health data via wearable devices or observing, monitoring or controlling individuals, including data collected through networks e.g. employees' activities, including the monitoring of the employees' work station, internet activity; closed circuit television; connected devices e.g. smart meters, smart cars, home automation; includes internet tracking and profiling for behavioural advertisement?	Yes|No|Not Sure	Under Data Protection legislation, organisations are obliged to demonstrate that their processing activities are compliant with the Data Protection Principles. Data Protection Impact Assessments are a tool designed to enable organisations to work out the risks that are inherent in proposed data processing activities before those activities commence. This enables organisations to address and mitigate those risks before the processing begins. A Data Protection Impact Assessment is required for any intended processing listed in the table below. If all your responses in the screening questionnaire are "No", this indicates that a documented Data Protection Impact Assessment Report is NOT required. If one or more of your responses in the screening questionnaire are "Yes", this indicates that a documented Data Protection Impact Assessment Report IS required.

You/your organisation's "intended processing involves sensitive information or information of a highly personal nature e.g. health" i.e. physical / mental health or condition (past, current or future status) including: •Medical data – data that are inherently / clearly medical data •Raw sensor data – data that can be used by itself or in combination with other data to draw a conclusion about the actual health status or health risk of a person •Conclusions data – data where conclusions are drawn about a person's health status or health risk, irrespective of whether these conclusions are accurate, or otherwise adequate.	Yes|No|Not Sure	
You/your organisation's intended processing involves evaluation or scoring including profiling & predicting using information about a person?	Yes|No|Not Sure	
You/your organisation's intended processing involves any automated decision making which has a legal or similar legal effect e.g. whether to employ an individual, grant them a loan or offer medical insurance?	Yes|No|Not Sure	
You/your organisation's intended processing involves personal data processed on a large scale . **For the purposes of NHS Apps and wearables programme, "large scale" is 2000 or more (or expected to reach 2000 or more) individuals.**	Yes|No|Not Sure	
You/your organisation's intended processing involves matching or combining of datasets? i.e. matching two or more data processing operations performed for different purposes in a way that would exceed the reasonable expectations of an individual.	Yes|No|Not Sure	
You/your organisation's intended processing involves data concerning vulnerable individuals who may be unable to easily consent or oppose the processing, or exercise their rights? This group may include children (incl babies), employees, mentally ill persons, asylum seekers, or the elderly, patients and cases where an imbalance in the relationship between the position of the individual and the controller can be identified.	Yes|No|Not Sure	
You/your organisation's the intended processing involves innovative use or applying new technological or organisational solutions e.g. combining use of finger print and face recognition for improved physical access control?	Yes|No|Not Sure	
You/your organisation's intended processing involves processing which in itself 'prevents data subjects from exercising a right or using a service or contract' e.g. determining eligibility based on an individual's circumstances?	Yes|No|Not Sure	
If one or more of your responses in the screening questionnaire are "Not sure", please check the guidance on ICO's website (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/). Please confirm that you have visited ICO's website	Yes|No	
If, after visiting the ICO website, you are still not sure then please describe the situation here, submit your questionnaire and request our guidance before continuing.		
If you have answered YES to any of these screening questions, then you are required to complete a full DPIA.		

You/your organisation has a FULLY documented Data Protection Impact Assessment Report for the intended processing which covers all the criteria for an acceptable DPIA set out in European guidelines.	Yes|No|Not Sure	The criteria needed for an acceptable DPIA are set out in European guidelines- See Annex 2 of: http://ec.europa.eu/newsroom/document.cfm?doc_id=47711 A DPIA template is available from the ICO website – see: PDF - https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf WORD - https://ico.org.uk/media/for-organisations/documents/2258857/dpia-template-v1.docx

Assessment stage 3 - Data Protection (Controllers only)

This section requests Controllers (only) to complete the ICO Controller checklist (a tool to assess general compliance with d ata protection law and identify if adequate measures are in place to keep people's personal data secure).

Section	Category	Question	Response	Relevant Guidance
Data Protection	ICO Data protection assurance checklists	Please complete the **Controllers checklist** on the ICO website and answer the questions below. What was your overall grading? Note: You must achieve an overall rating of Green or Amber to be considered	Red Amber Green	Data protection self assessment: **Controllers checklist** https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/
Data Protection	ICO Data protection assurance checklists	How many were rated "Not yet implemented or planned"?		
Data Protection	ICO Data protection assurance checklists	How many were rated "Partially implemented or planned"?		
Data Protection	ICO Data protection assurance checklists	How many were rated "Successfully implemented"?		
Data Protection	ICO Data protection assurance checklists	How many were rated "Not applicable"?		
Data Protection	ICO Data protection assurance checklists	Who completed the ICO Controller Checklist?		
Data Protection	ICO Data protection assurance checklists	What date was this checklist completed on?		

NHS Digital Assessment stage 4 - Data Protection - Advanced questions

This section is a comprehensive compliance checklist which should be completed by Controllers (to which the data protection law directly applies).

Question	Response	Relevant Guidance
The legal basis for each processing purpose of the personal data is clearly described to the individual	Yes|No|Not Applicable	
The legal basis for the processing of personal data is …	Consent|Other legal basis| Not Sure	
The legal basis for each processing purpose processing of sensitive personal data is clearly described to the individual	Yes|No|Not Sure|Not Relevant	
The legal basis for the processing of sensitive personal data is …	Consent|Other legal basis| Not Sure	
If you have responded "Not sure" to any of the questions, please check the guidance on ICO's website (https://ico.org.uk/). Please confirm that you have visited ICO's website	Yes|No	
If, after visiting the ICO website, you are still not sure then please describe the situation here, submit your questionnaire and request our guidance before continuing.		
You/your organisation has identified and documented the required actions to a breach before a breach occurs.	Yes|No	A breach occurs when personal data is subjected to an incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, that personal data.
If 5d.7=Yes ,the actions needed to evaluate and decide: • whether personal data is involved • notification to the Data Protection Authority (in UK the ICO) without undue delay and, not later than 72 hours • the technical and organisational protection measures • your subsequent measures to ensure that the high risk to the rights and freedoms of app users is no longer likely • notification to affected individuals without undue delay of the appropriate details e.g. likely consequences; your measures to mitigate possible adverse effects	Yes|No|Not Sure|Not Applicable	
If you have responded "Not sure" to any of the questions, please check the guidance on ICO's website (https://ico.org.uk/). Please confirm that you have visited ICO's website	Yes|No	
If, after visiting the ICO website, you are still not sure then please describe the situation here, submit your questionnaire and request our guidance before continuing.		

You/your organisation has developed measures contributing to the rights of the data subjects	Yes|No|Not Sure	UK/EU data protection legislation enacted in 2018 extends individuals' rights. Controllers need to be able to demonstrate compliance not only when individuals seek to exercise those rights. Individuals must be able to exercise their rights free of charge, and a controller obtaining a request in connection with an individual right must comply without undue delay i.e. within one month or with a maximum two month extension if the request is complex/high number of requests.
If 'yes', then the rights of the data subjects include- · providing information provided to the data subject	Yes|No|Not Sure|Not Applicable	
If 'yes', then the rights of the data subjects include - · right of access	Yes|No|Not Sure|Not Applicable	
If 'yes', then the rights of the data subjects include - · right of access	Yes|No|Not Sure|Not Applicable	
If 'yes', then the rights of the data subjects included - · right of data portability (only applies where consent or contract with the data subject is the legal basis and personal data are: o 'knowingly and actively provided by the data subject' o 'generated by and collected from the use of the service or device' (i.e. 'observed' such as search history, traffic data, location data, other raw data such as heartbeat tracked by fitness and health trackers.	Yes|No|Not Sure|Not Applicable	
If 'yes', then the rights of the data subjects included - · right to erase (or the "right to be forgotten)	Yes|No|Not Sure|Not Applicable	
If 'yes', then the rights of the data subjects included - · right to rectify, object, restrict processing	Yes|No|Not Sure|Not Applicable	
If you have responded "Not sure" to any of the questions, please check the guidance on ICO's website (https://ico.org.uk/). Please confirm that you have visited ICO's website	Yes|No	
If, after visiting the ICO website, you are still not sure then please describe the situation here, submit your questionnaire and request our guidance before continuing.		
You/your organisation use all reasonable measures to verify the identity of an individual who exercises these rights	Yes|No|Not Sure	

You/your organisation make personal data available to a 3rd party which:	Yes|No, no 3rd party processes personal data| Not sure	This section focuses on the legal requirement that a Controller has an appropriate written contract in place with a Processor (3rd party that processes personal data on behalf of the controller). Under data protection, “Controllers” have more liability than “Processors” i.e.: • Controllers are liable for all damage caused by processing which infringes the legislation • Processors are liable when they breach processor-specific provisions or act outside the Controller’s instructions set out in a processing contract A Controller that uses a ‘Processor’ must, by UK/EU law, have a binding legal agreement in place that sets out each party’s respective obligations, responsibilities and liabilities. Controllers should not accept liability clauses where Processors are indemnified against fines or claims under UK/EU law as this would undermine the principles whereby the legal penalty regime extends directly to Processors to ensure better performance and enhanced protection. A Controller must only use a processor that can provide “sufficient guarantees” in terms of its resources and expertise, to implement technical and organisational measures to comply with the UK/EU data protection legislation and protect the rights of data subjects.
If 'yes', the 3rd party provides technical services e.g.: maintains data backups or stores data in a cloud	Yes|No|Not Sure|Not Applicable	
If 'yes', the 3rd party provides non-technical services e.g. analyses data collected via the tool/app.	Yes|No|Not Sure|Not Applicable	
If 5d.10 =Yes , A written binding agreement e.g. contract is in place between you/your organisation and each processor.	Yes|No|Not Sure|Not Applicable	
If 5d.10= Yes, No contract clauses indemnify Processors against fines or claims under UK/EU data protection law	Yes|No|Not Sure|Not Applicable	
If 5d.10=Yes, All the processing contracts clearly set out the subject matter and duration of the processing	Yes|No|Not Sure|Not Applicable	
If 5d.10=Yes, All the processing contracts clearly set out the nature and purpose of the processing	Yes|No|Not Sure|Not Applicable	

If 5d.10=Yes, All the processing contracts clearly set out: · the type of personal data and categories of data subject	Yes|No|Not Sure|Not Applicable	
If 5d.10=Yes, All the processing contracts clearly set out the obligations and rights of the controller	Yes|No|Not Sure|Not Applicable	
If 5d.10=Yes, All the processing contracts require the processor to only act on the written instructions of the controller	Yes|No|Not Sure|Not Applicable	
If 5d.10=Yes, All the processing contracts require the processor to ensure that people processing the data are subject to a duty of confidence	Yes|No|Not Sure|Not Applicable	
If 5d.10=Yes, All the processing contracts require the processor to take appropriate measures to ensure the security of processing	Yes|No|Not Sure|Not Applicable	
If 5d.10=Yes, All the processing contracts require the processor to only engage sub-processors with the prior consent of the controller and under a written contract	Yes|No|Not Sure|Not Applicable	
If 5d.10=Yes, All the processing contracts require the processor to assist the controller in providing subject access and allowing data subjects to exercise their rights under the UK/EU law	Yes|No|Not Sure|Not Applicable	
If 5d.10=Yes, All the processing contracts require the processor to: • assist the controller in meeting its UK/EU data protection law obligations in relation to: o the security of processing o the notification of personal data breaches and o data protection impact assessments	Yes|No|Not Sure|Not Applicable	
If 5d.10=Yes, All the processing contracts require the processor to delete or return all personal data to the controller as requested at the end of the contract	Yes|No|Not Sure|Not Applicable	
If 5d.10=Yes, All the processing contracts require the processor to submit to audits and inspections	Yes|No|Not Sure|Not Applicable	
If 5d.10=Yes, All the processing contracts require the processor to provide the controller with whatever information it needs to ensure that they are both meeting their obligations	Yes|No|Not Sure|Not Applicable	
If 5d.10=Yes, All the processing contracts require the processor to tell the controller immediately if it is asked to do something infringing UK/EU data protection law	Yes|No	
If, after visiting the ICO website, you are still not sure then please describe the situation here, submit your questionnaire and request our guidance before continuing.		
Consent is freely given, specific for each purpose and informed	Yes|No|Not Sure	Consent is defined as “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”

Consent is not a precondition of signing up to a service, unless it is necessary for that service.	Yes|No|Not Sure	
Consent is requested separate from the terms and conditions	Yes|No|Not Sure	
If 5d.14=Yes, then at the time consent is requested, the individual is informed of: · the controller's identity and the names of any third parties who will receive the personal data	Yes|No|Not Sure|Not Applicable	
If 5d.14=Yes, then at the time consent is requested, the individual is informed of: · the purpose of each of the processing operations for which consent is sought	Yes|No|Not Sure|Not Applicable	
If 5d.14=Yes, then at the time consent is requested, the individual is informed of: · the type of personal data (e.g. IP address) which will be collected and used	Yes|No|Not Sure|Not Applicable	
If 5d.14=Yes, then at the time consent is requested, the individual is informed of: · the existence of the right to withdraw consent at any time they wish	Yes|No|Not Sure|Not Applicable	
If 5d.14=Yes, then at the time consent is requested, the individual is informed of: · (if applicable) the use of the data for decisions based solely on automated processing, including profiling	Yes|No|Not Sure|Not Applicable|Not Relevant	
If 5d.14=Yes, then at the time consent is requested, the individual is informed of: · (If applicable) for consent that relates to transfers; the possible risks of data transfers to third countries in the absence of an adequacy decision (the recipient country is recognised by the EU Commission to have an adequate level of protection) and appropriate safeguards	Yes|No|Not Sure|Not Applicable|Not Relevant	
The individual can withdraw consent as easily as it was given e.g. via the same electronic interface, an unsubscribe link; instructions in emails contained in all communications	Yes|No|Not Sure	
Consent (granular consent) is obtained separately for every type of purpose foreseen e.g. marketing	Yes|No|Not Sure|Not Relevant	
If a future additional purpose is envisaged after consent was obtained and the new purpose is incompatible with the original purpose, then additional; consent is obtained for the new purpose	Yes|No|Not Sure|Not Relevant	
Consent is recorded	Yes, for the current consent only|Yes, for current and previous consents|No|Not Relevant	
You/your organisation can evidence that the individual gave their valid consent to the processing i.e. how and when consent was obtained and the information provided to the individual (data subject) at the time	Yes|No|Not Sure	
The individual is required to provide a clear affirmative action to signify consent to the processing of personal data for each purpose	Yes, by an opt button or link online|Yes, by selecting from equally prominent yes/no options|Yes, by responding to an email requesting consent|Yes, by filling optional fields in a form|Yes, Other|No/Not Sure	
You/your organisation confirms it does NOT use:		
· pre-ticked opt-in boxes or	Yes|No|Not Sure	
· blank opt-out boxes or	Yes|No|Not Sure	
· default settings or	Yes|No|Not Sure	
· a blanket acceptance of your terms and conditions	Yes|No|Not Sure	
You/your organisation ensures that the individual can refuse to consent without detriment	Yes|No|Not Sure	
You/your organisation does not penalise individuals who withdraw consent	Yes|No|Not Sure	

If you have responded “Not sure” to any of the questions, please check the guidance on ICO's website (https://ico.org.uk/). Please confirm that you have visited ICO's website	Yes|No	
If, after visiting the ICO website, you are still not sure then please describe the situation here, submit your questionnaire and request our guidance before continuing.		
Traditionally, data was collected directly from individuals e.g. when they filled in a form. Increasingly, organisations use data that has not been consciously provided by individuals in this way. It may be: • observed, by tracking people online or by smart devices; • derived from combining other data sets; or • inferred by using algorithms to analyse a variety of data, such as location data, records of purchases in order to profile people for credit risk, state of health or suitability for a job As a Controller you have a ‘duty of transparency’ which means providing information to people about how, why and when you process their personal data. This information must be: • concise, transparent, intelligible and easily accessible • written in clear and plain language, particularly if addressed to a child and • free of charge		
How is the personal data obtained?		
The personal data is obtained directly from the individual (data subject)	Yes|No|Not Sure	
If 5d.31=Yes, Identity and contact details of the Controller and where applicable, the Controller’s representative).	Yes|No|Not Sure|Not Applicable	
If 5d.31=Yes, Purposes of processing and the legal basis for processing.	Yes|No|Not Sure|Not Applicable	
If 5d.31=Yes, Recipients or categories of recipients of the personal data.	Yes|No|Not Sure|Not Applicable	
If 5d.31=Yes, Details of data transfers outside the European Economic Area, including how the data will be protected e.g.: • The recipient is in an ‘adequate’ country i.e. recognised by the EU Commission to have an adequate level of protection • Binding Corporate Rules (BCR) or • Model Contract Clauses and you have made the individual aware of how they may obtain a copy of the BCRs or other safeguards, or where such safeguards have been made available.	Yes|No|Not Sure|Not Applicable|Not Relevant	
If 5d.31=Yes, The retention period or, if no fixed retention period can be provided – the criteria used to determine that period.	Yes|No|Not Sure|Not Applicable	
If 5d.31=Yes, The right to lodge a complaint with a supervisory authority (in the UK this would be the Information Commissioner (ICO)).	Yes|No|Not Sure|Not Applicable	
If 5d.31=Yes, (if relevant) Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data.	Yes|No|Not Sure|Not Applicable|Not Relevant	

If 5d.31=Yes, (if relevant) The existence of automated decision making including profiling and information about how decisions are made, the significance and the consequences.	Yes|No|Not Sure|Not Applicable|Not Relevant	
If 5d.31=Yes, The existence of the data subject's right: · to access his/her personal data.	Yes|No|Not Sure|Not Applicable	
If 5d.31=Yes, The existence of the data subject's right: · to rectify, erase and restrict his/her personal data.	Yes|No|Not Sure|Not Applicable	
If 5d.31=Yes, The existence of the data subject's right: · to object to the processing.	Yes|No|Not Sure|Not Applicable	
If 5d.31=Yes, (if relevant) The existence of the data subject's right: · to withdraw consent.	Yes|No|Not Sure|Not Applicable	
If 5d.31=Yes, (if relevant) The existence of the data subject's right: · to data portability (provide the personal data in machine readable form).	Yes|No|Not Sure|Not Applicable	
If 5d.31=Yes, (if relevant) The existence of the data subject's right: · to object to decisions based solely on automated processing (which could include profiling), if the decisions produce legal effects or similarly significantly affects the data subject.	Yes|No|Not Sure|Not Applicable	
If 5d.31=Yes, This transparency information is provided free of charge.	Yes|No|Not Sure|Not Applicable	
If 5d.31=Yes, If the personal data is later to be used for a new lawful purpose which was not adequately described in the initial transparency information and is "not incompatible" with the original purpose - you will provide updated transparency information which may mean re-obtaining consent (if consent was the lawful basis).	Yes|No|Not Sure|Not Applicable	
If 5d.31=Yes, The transparency information is provided at the time the personal data are obtained.	Yes|No|Not Sure|Not Applicable	
If 5d.31=Yes, Are changes to the existing transparency information notified to users and consent obtained again (unless the consent obtained previously remains valid).	Yes|No|Not Sure|Not Applicable	
Personal data is NOT obtained directly from the individual (data subject)"	Yes|No|Not Sure	
If 5d.32 =Yes, Identity and contact details of the Controller and where applicable, the Controller's representative).	Yes|No|Not Sure|Not Applicable	
If 5d.32 =Yes, Purposes of processing and the legal basis for processing.	Yes|No|Not Sure|Not Applicable	
If 5d.32 =Yes, Categories of personal data.	Yes|No|Not Sure|Not Applicable	
If 5d.32 =Yes, The source the personal data originates from and whether it came from publicly accessible sources.	Yes|No|Not Sure|Not Applicable	
If 5d.32 =Yes, Recipients or categories of recipients of the personal data.	Yes|No|Not Sure|Not Applicable	
If 5d.32 =Yes, Details of data transfers outside the European Economic Area, including how the data will be protected e.g.: • The recipient is in an 'adequate' country i.e. recognised by the EU Commission to have an adequate level of protection • Binding Corporate Rules (BCR) or • Model Contract Clauses and you have made the individual aware of how they may obtain a copy of the BCRs or other safeguards, or where such safeguards have been made available.	Yes|No|Not Sure|Not Applicable|Not Relevant	

If 5d.32 =Yes, The retention period or, if no fixed retention period can be provided – the criteria used to determine that period.	Yes|No|Not Sure|Not Applicable	
If 5d.32 =Yes, The right to lodge a complaint with a supervisory authority (in the UK this would be the Information Commissioner (ICO)).	Yes|No|Not Sure|Not Applicable	
If 5d.32 =Yes, (if relevant) The existence of automated decision making including profiling and information about how decisions are made, the significance and the consequences.	Yes|No|Not Sure|Not Applicable|Not Relevant	
If 5d.32 =Yes, The existence the data subject's right: · to access his/her personal data.	Yes|No|Not Sure|Not Applicable	
If 5d.32 =Yes, The existence the data subject's right: · to rectify, erase and restrict his/her personal data.	Yes|No|Not Sure|Not Applicable	
If 5d.32 =Yes, The existence of the data subject's right: · to object to the processing.	Yes|No|Not Sure|Not Applicable	
If 5d.32 =Yes, The right to object to processing of personal data is communicated to the data subject no later than the time of the first communication with the data subject and the information is provided clearly and separately from any other information provided to the data subject.	Yes|No|Not Sure|Not Applicable	
If 5d.32 =Yes, (if relevant) The existence of the data subject's right: · to withdraw consent	Yes|No|Not Sure|Not Applicable|Not Relevant	
If 5d.32 =Yes, (if relevant) The existence of the data subject's right: · data portability (provide the personal data in machine readable form)	Yes|No|Not Sure|Not Applicable|Not Relevant	
If 5d.32 =Yes, (if relevant) The existence of the data subject's right: · to object to decisions based solely on automated processing (which could include profiling), if the decisions produce legal effects or similarly significantly affects the data subject	Yes|No|Not Sure|Not Applicable|Not Relevant	
If 5d.32 =Yes, This transparency information is provided free of charge	Yes|No|Not Sure|Not Applicable	
If 5d.32 =Yes, If the personal data is later to be used for a new lawful purpose which was not adequately described in the initial transparency information and is "not incompatible" with the original purpose - you will provide updated transparency information (and consent if consent was the lawful basis).	Yes|No|Not Sure|Not Applicable	
If 5d.32 =Yes, The transparency information is provided within one month of having obtained the data OR if the data are used to communicate with the individual, at the latest, when the first communication takes place.	Yes|No|Not Sure|Not Applicable	
If 5d.32 =Yes, If disclosure to another recipient is envisaged, the transparency information is provided, at the latest, before the data are disclosed.	Yes|No|Not Sure|Not Applicable	
If 5d.32 =Yes, Are changes to the existing transparency information notified to users and consent obtained again (unless the consent obtained previously remains valid).	Yes|No|Not Sure|Not Applicable	
If you have responded "Not sure" to any of the questions, please check the guidance on ICO's website (https://ico.org.uk/). Please confirm that you have visited ICO's website	Yes|No	
If, after visiting the ICO website, you are still not sure then please describe the situation here, submit your questionnaire and request our guidance before continuing.		
You/your organisation's digital tools/app are particularly aimed at children	Yes|No|Not Sure	
You/your organisation's digital tools/app are particularly likely to be used by children	Yes|No|Not Sure	

If 5d.35 & 5d.36=No, then please skip this section or else Complete the child's data protection rights. You/your organisation:		
· Processes by which a child can exercise their data protection rights are designed with the child in mind and make them easy for children to access and understand.	Yes|No|Not Sure|Not Applicable	
· Allow competent children to exercise their own data protection rights.	Yes|No|Not Sure|Not Applicable	
· If our original processing was based on consent provided when the individual was a child, then you comply with requests for erasure whenever you can.	Yes|No|Not Sure|Not Applicable	
· You/your organisation design your processes so that, as far as possible, it is as easy for a child to get their personal data erased as it was for them to provide it in the first place.	Yes|No|Not Sure|Not Applicable	
General. You/your organisation:		
· Complies with all the requirements of the UK/EU data protection legislation, not just those specifically relating to children and included in this checklist.	Yes|No|Not Sure|Not Applicable	
· Designs your processing with children in mind from the outset and use a data protection by design and by default approach.	Yes|No|Not Sure|Not Applicable	
· Makes sure that your processing is fair and complies with the data protection principles.	Yes|No|Not Sure|Not Applicable	
· As a matter of good practice, you use DPIAs to help us assess and mitigate the risks to children.	Yes|No|Not Sure|Not Applicable	
· If your processing is likely to result in a high risk to the rights and freedom of children then we always do a DPIA.	Yes|No|Not Sure|Not Applicable	
· As a matter of good practice, you consult with children as appropriate when designing our processing.	Yes|No|Not Sure|Not Applicable	
Privacy notices. You/your organisation:		
· Provide privacy notices which are clear, and written in plain, age-appropriate language.	Yes|No|Not Sure|Not Applicable	
· Use child friendly ways of presenting privacy information, such as: diagrams, cartoons, graphics and videos, dashboards, layered and just-in-time notices, icons and symbols.	Yes|No|Not Sure|Not Applicable	
· Explain to children why you require the personal data you have asked for, and what you will do with it, in a way which they can understand.	Yes|No|Not Sure|Not Applicable	
· As a matter of good practice, you explain the risks inherent in the processing, and how you intend to safeguard against them, in a child friendly way, so that children (and their parents) understand the implications of sharing their personal data.	Yes|No|Not Sure|Not Applicable	
· Tell children what rights they have over their personal data in language they can understand.	Yes|No|Not Sure|Not Applicable	
· As a matter of good practice, if relying upon parental consent then you offer two different versions of your privacy notices; one aimed at the holder of parental responsibility and one aimed at the child.	Yes|No|Not Sure|Not Applicable	
Basis for processing a child's personal data. You/your organisation:		
· When relying on consent, make sure that the child understands what they are consenting to, and you do not exploit any imbalance in power in the relationship between you and the child.	Yes|No|Not Sure|Not Applicable	
· When relying on 'necessary for the performance of a contract', you consider the child's competence to understand what they are agreeing to, and to enter into a contract.	Yes|No|Not Sure|Not Applicable	
· When relying upon 'legitimate interests', you take responsibility for identifying the risks and consequences of the processing, and put age appropriate safeguards in place.	Yes|No|Not Sure|Not Applicable	
Solely automated decision making (including profiling). You/your organisation:	Yes|No|Not Sure|Not Applicable	
· Do not usually use children's personal data to make solely automated decisions about them if these will have a legal, or similarly significant effect upon them.	Yes|No|Not Sure|Not Applicable	

· If you do use children's personal data to make such decisions then we make sure that one of the exceptions applies and that suitable, child appropriate, measures are in place to safeguard the child's rights, freedoms and legitimate interests.	Yes|No|Not Sure|Not Applicable	
· In the context of behavioural advertising, when deciding whether a solely automated decision has a similarly significant effect upon a child, you take into account: the choices and behaviours that you are seeking to influence; the way in which these might affect the child; and the child's increased vulnerability to this form of advertising; using wider evidence on these matters to support our assessment.	Yes|No|Not Sure|Not Applicable	
· Stop any profiling of a child that is related to direct marketing if they ask you to.	Yes|No|Not Sure|Not Applicable	
Marketing. You/your organisation:		
· When considering marketing to children you take into account their reduced ability to recognise and critically assess the purposes behind the processing and the potential consequences of providing their personal data.	Yes|No|Not Sure|Not Applicable	
· Take into account sector specific guidance on marketing, to make sure that children's personal data is not used in a way that might lead to their exploitation.	Yes|No|Not Sure|Not Applicable	
· Stop processing a child's personal data for the purposes of direct marketing if they ask you to.	Yes|No|Not Sure|Not Applicable	
· Comply with the direct marketing requirements of the Privacy and Electronic Communications Regulations (PECR).	Yes|No|Not Sure|Not Applicable	
Offering an information Society Service (ISS) directly to a child, on the basis of consent. You/your organisation:		
· If you decide not to offer your ISS (online service) directly to children, then you mitigate the risk of them gaining access, using measures that are proportionate to the risks inherent in the processing.	Yes|No|Not Sure|Not Applicable	
· When offering ISS to UK children on the basis of consent, you make reasonable efforts (taking into account the available technology and the risks inherent in the processing) to ensure that anyone who provides their own consent is at least 13 years old.	Yes|No|Not Sure|Not Applicable	
· When offering ISS to UK children on the basis of consent, you obtain parental consent to the processing for children who are under the age of 13, and make reasonable efforts (taking into account the available technology and risks inherent in the processing) to verify that the person providing consent holds parental responsibility for the child.	Yes|No|Not Sure|Not Applicable	
· When targeting wider European (non UK) markets you comply with the age limits applicable in each Member state.	Yes|No|Not Sure|Not Applicable	
· You regularly review available age verification and parental responsibility verification mechanisms to ensure you are using appropriate current technology to reduce risk in the processing of children's personal data.	Yes|No|Not Sure|Not Applicable	
· You do not seek parental consent when offering online preventive or counselling services to a child.	Yes|No|Not Sure|Not Applicable	
If you have responded "Not sure" to any of the questions, please check the guidance on ICO's website (https://ico.org.uk/). Please confirm that you have visited ICO's website	Yes|No	
If, after visiting the ICO website, you are still not sure then please describe the situation here, submit your questionnaire and request our guidance before continuing.		
You/your organisation use cookies, web beacons etc	Yes|No|Not Sure	
If 5d.79=Yes, you provide users with a cookie policy	Yes|No|Not Sure|Not Applicable	

If 5d.80=Yes, the cookie policy … · explains that consent is being requested for the storage and access of cookies in and from the users' terminal equipment?	Yes|No|Not Sure|Not Applicable	
If 5d.80=Yes, the cookie policy … · ensures consent is valid by being demonstrated by a clear affirmative action from the user (i.e. silence, pre-ticked boxes or inactivity do not constitute valid consent).	Yes|No|Not Sure|Not Applicable	
If 5d.80=Yes, the cookie policy … · fully explains the purpose, in plain language, of each cookie type being used?	Yes|No|Not Sure|Not Applicable	
You use 'strictly necessary' cookies (without which the end user would be unable to use the specific service explicitly requested)?	Yes|No|Not Sure|Not Applicable	
If 5d.81=Yes, Although consent is not required, is the end user made aware that strictly necessary' cookies are being used?	Yes|No|Not Sure|Not Applicable	
If 5d.81=Yes,Consent recorded for each separate cookie purpose?	Yes|No|Not Sure|Not Applicable	
If 5d.81 & 5d.82=Yes, You/your organisation can evidence that the individual gave their valid consent to the processing i.e. how and when consent was obtained and the information provided to the individual (data subject) at the time	Yes|No|Not Sure|Not Applicable	
If 5d.81=Yes,The user able to withdraw consent as easily as it was given e.g. via the same electronic interface?	Yes|No|Not Sure|Not Applicable|Not Relevant	
If you have responded "Not sure" to any of the questions, please check the guidance on ICO's website (https://ico.org.uk/). Please confirm that you have visited ICO's website	Yes|No	
If, after visiting the ICO website, you are still not sure then please describe the situation here, submit your questionnaire and request our guidance before continuing.		
Do you collect usage or bug report data?	Yes|No|Not Sure	
If 5d.86=Yes, · Is this collected with informed consent from the user	Yes|No|Not Sure|Not Applicable	
If 5d.86=Yes · Is this collected using anonymised data (so that no personal data is collected)	Yes|No|Not Sure|Not Applicable	
If you have responded "Not sure" to any of the questions, please check the guidance on ICO's website (https://ico.org.uk/). Please confirm that you have visited ICO's website	Yes|No	
If, after visiting the ICO website, you are still not sure then please describe the situation here, submit your questionnaire and request our guidance before continuing.		

You/your organisation’s core activities consist of processing operations which requires the processing on a large scale of special categories of data such as health data.	Yes|No|Not Sure	Under UK/EU data protection legislation, an organisation must appoint a Data Protection Officer if you/your organisation: • is a public authority (except for courts acting in their judicial capacity) • carries out large scale systematic monitoring of individuals (for example, online behaviour tracking) or • carries out large scale processing of sensitive personal data (also know as special categories of data) e.g. health data
You/your organisation’s core activities consist of processing operations which requires regular and systematic monitoring of data subjects on a large scale.	Yes|No|Not Sure	
You/your organisation has a designated Data Protection Officer who is formally tasked with ensuring that you/your organisation is aware of, and complies with, its data protection responsibilities.	Yes|No|Not Sure	
If you have responded “Not sure” to any of the questions, please check the guidance on ICO's website (https://ico.org.uk/). Please confirm that you have visited ICO's website	Yes|No	
If, after visiting the ICO website, you are still not sure then please describe the situation here, submit your questionnaire and request our guidance before continuing.		

Assessment stage - Security

For developers to demonstrate compliance with OWASP standards for Security.

Category	Question	Response	Relevant Guidance
Please choose the right standard	What type of Apps or Digital Tool is being assessed 1. Web application or /and Native desktop application 2. Mobile application 3. Both (1&2)		
Web application or /and Native desktop application	Please indicate current Level: Architecture, Design and Threat Modelling	Level:	https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
Web application or /and Native desktop application	Please indicate current Level: Authentication	Level:	
Web application or /and Native desktop application	Please indicate current Level: Session management	Level:	
Web application or /and Native desktop application	Please indicate current Level: Access control	Level:	
Web application or /and Native desktop application	Please indicate current Level: Malicious input handling	Level:	
Web application or /and Native desktop application	Please indicate current Level: Cryptography at rest	Level:	
Web application or /and Native desktop application	Please indicate current Level: Error handling and logging	Level:	
Web application or /and Native desktop application	Please indicate current Level: Data protection	Level:	
Web application or /and Native desktop application	Please indicate current Level: Communications	Level:	
Web application or /and Native desktop application	Please indicate current Level: HTTP security configuration	Level:	

Web application or /and Native desktop application	Please indicate current Level: Malicious controls	Level:	
Web application or /and Native desktop application	Please indicate current Level: Business logic	Level:	
Web application or /and Native desktop application	Please indicate current Level: File and resources	Level:	
Web application or /and Native desktop application	Please indicate current Level: Web services (NEW for 3.0)	Level:	
Web application or /and Native desktop application	Please indicate current Level: Configuration (NEW for 3.0)	Level:	
Mobile App	Please indicate current Level: Architecture, Design and Threat Modelling	Level:	https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide
Mobile App	Please indicate current Level: Data Storage and Privacy	Level:	
Mobile App	Please indicate current Level: Cryptography	Level:	
Mobile App	Please indicate current Level: Authentication and Session Management	Level:	
Mobile App	Please indicate current Level: Network Communication	Level:	
Mobile App	Please indicate current Level: Platform Interaction	Level:	
Mobile App	Please indicate current Level: Code Quality and Build Setting	Level:	
Mobile App	Please indicate current Level: Resilience	Level:	
		Level:	

Assessment stage - Usability & Accessibility

For developers to demonstrate adherence to user centred design for use in health and social care.

Question	Response	Relevant Guidance
Does the colour contrast of the text on your native app comply with WCAG 2.0 AA level requirements?	Yes|No	To be considered for the apps library, all text in your app must have a contrast ratio of at least 4.5:1 as detailed in the WCAG guideline 1.4.3 https://www.w3.org/TR/UNDERSTANDING-WCAG20/visual-audio-contrast-contrast.html
Did you follow the 6 key principles under the user centred design (UCD) process that conforms to the ISO 9241-210 standard?	Yes|No	
What phases did your user-centered design process go through - for example discovery, alpha, beta, go live?		
What user demographics were defined at the outset of app development?		
Was a representative/suitable sample of this user demographic engaged with throughout the user centred design process?	Yes|No	
What user needs were captured/confirmed through the engagement of users?		
Were the user needs recorded in a clear technology neutral format for example in user stories?	Yes|No	
For each of the user needs were clear user acceptance criteria defined?	Yes|No	
Were the user needs and user stories the basis upon which the apps were developed?	Yes|No	
Please explain why, and describe where the development focus differs from identified user needs		
How many times were early versions of the app evaluated with a sample of the user demographic?		
Before release was the app evaluated with a representative sample of the user demographic?	Yes|No	
Throughout the evaluation of early versions and pre-release versions what changes were made to the app in light of the user feedback? Please provide examples/evidence.		
Post-release, how do you continue to collect feedback from users and make changes to the app based on this feedback?		
What is your post-release schedule of improvements for the app?		
Is your application a native iOS or Android app?	Yes|No	

What device OS accessibility features does your app use? e.g. VoiceOver (iOS), Dynamic Type (iOS), TalkBack (Android) or Select To Speak (Android)		
What steps have been taken to minimise battery usage?		
Is your application a progressive web app?	Yes|No	https://developers.google.com/web/progressive-web-apps/checklist
Your progressive web app ~~should~~ comply with the baseline checklist for progressive web apps, as defined by Google		https://developers.google.com/web/progressive-web-apps/checklist
Please list any items on this checklist, which your progressive web app does not meet.		
Have you conducted accessibility testing on your progressive web app?	Yes|No	
Please provide evidence of this, including outcomes and any planned further changes to improve accessibility.		
Is your application a web-based tool/service? or if you are submitting a native app that has an associated web service which handles user data	Yes|No	
Is the website responsive?	Yes|No	Only answer these questions, if your submission is for a web-based tool/service, or if you are submitting a native app that has an associated web service which handles
Does your web service conform to WCAG 2.0 and other W3C/WAI guidelines on accessibility?	Yes|No	
Does your web service provide text equivalents for every non-text element within the app?	Yes|No	
Does your web service provide an accessibility statement?	Yes|No	
Please provide a link to your accessibility statement		
Have you conducted accessibility testing on your web service?	Yes|No	
Please provide evidence of this, including outcomes and any planned further changes to improve accessibility.		
Can your web service be used with screen readers or other assistive technologies?	Yes|No	

Assessment stage - Interoperability

For developers to demonstrate adherence to interoperability standards.

Category	Question	Response	Relevant Guidance
Data Formats	Provide details of any Proprietary Formats which are used to store or transfer data - specify whether these are open/published or closed		If data stored in Propietary Formats this can have a number of implications such as ease of access to the data by any other legitimate parties and interoperability.
Exposure of API's	Does your solution expose any API's or Integration Channels for other Consumers?	Yes|No|Not applicable	
Exposure of API's	If 'yes', Does your API adhere to the Government Digital Services (GDS) Open API Best Practices	Yes|No	Best Practice link: https://www.gov.uk/guidance/gds-api-technical-and-data-standards
Exposure of API's	If there are specific areas where best practices are not followed please list the rationale and relevant mitigations put in place		
Exposure of API's	if 'no', please state reasons and why they are not applicable		
Data Export	Is the Solution capable of exporting data in a standard format?	Yes|No	
Data Export	If 'no', Please state the reasons and relevant mitigations		
Consuming Data from other Sources	Does the Service consumes other API's or receives Data from other sources	Yes|No	Company/Datastore/healthcare Provider (eg. Other Clinical Systems or Apps or Drug Database)
Consuming Data from other Sources	If 'yes', state the different Systems or Sources from which information is obtained		
Consuming Data from other Sources	If 'yes', within the App Solution/Database is it possible to distinguish between information from different sources	Yes|No	
Consuming Data from other Sources	If 'no', state reason and relevant mitigation		
Medical Device Integration	Does your Solution consists of Wearables or Devices or integration with them	Yes|No	

Medical Device Integration	If 'yes', Please provide evidence of how it complies with - ISO/IEEE 11073 Personal Health Data (PHD) Standards		

Assessment stage - Technical Stability

NHS Digital

For developers to demonstrate approaches to technical stability.

Category	Question	Response
Quality Assurance	Are the source code and any configuration items for the digital service version controlled with all changes audited?	Yes|No
Quality Assurance	Do you have accreditation to any industry wide testing standards such as ISO 9001, ISO 29119 etc	Yes|No
Quality Assurance	Please state what testing accreditations you have or are in the process of acquiring (including completion dates)	
Quality Assurance	What levels of Testing is being executed for the digital service? with all significant issues identified in all test phases resolved prior to release.(If none of these, then reject)	1.Non-functional 2.Functional 3. Non -Fuctional & Functional 4. Regression 5. None
Quality Assurance	Please provide a brief outline of each of your testing activities (or provide documentation to support all of them)	
Quality Assurance	Please provide a reason why?	
Quality Assurance	Please provide a brief outline of your system for accepting and responding to technical faults from end users. (provide documentation to support this)	
Quality Assurance	Do you have the capacity to rollback to previous versions of the digital service as and when required.	Yes|No
Quality Assurance	Please provide a brief outline of your rollback process (or provide documentation to support this)	
Service Management	Do you proactively monitor running of systems and system components to automatically identify faults and technical issues?	Yes|No
Service Management	Please describe, your monitoring process & procedures	
Product Development	Do you have a documented roadmap for future digital service development?	Yes|No
Product Development	Do you have a plan for decommissioning the digital service?	Yes|No
Product Development	Please describe your procedures for decommissioning the service, dealing with any retained identifiable data?	
	Do you have a plan for dealing with any retained identifiable data in the event that the User stops using the service (e.g. uninstalls app or unsubscribes) ?	Yes|No
Product Development	Please describe your procedures?	