Privacy Impact Assessment - Risk Register
Initiative name: Covid-19 App (06/05/2020)

Mandatory privacy risks to assess - if not applicable place N/A with relevant detail to justify why it's not relevant. Also add further risks identified.

Risk reference: *A unique coding that allows the risk to be easily identified*	**Which elements of the initiative give rise to privacy risks?**	**What is/are the potential or actual privacy risk(s)**	**Risk Score**			**Proposed solution(s)/mitigating action(s) –** *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	**Result**	**Evaluation**	**Solution approved by**	**Action**	**Date for completion**	**Anticipated risk score**			**Responsibility**	**Current status/progress**
			Likelihood	**Impact**	**RAG status**							**Likelihood**	**Impact**	**RAG status**		
1	Transferring of data outside of the EEA	Non-compliance:- No adequacy arrangement results in serious non-compliance with the data protection legislation. This faces regulatory action and exposes the vulnerability of an organisation as it is a breach. If consequently there is any loss of personal data to non-trusted sources this is a further breach and risks privacy re onward sharing of personal data; reputational damage; loss of trust by data subjects.	2	2	AG	AWS - We're only using eu-west-2, so the data is located within the UK. Microsoft - fall back option Firebase - verify Pivotal - use our infrastructure										
2	Misuse of information by those with access	Non-compliance with the data protection legislation; vulnerability of organisation against breach and possible regulatory action; loss of personal data to non-trusted sources; privacy risk to onward sharing of personal data; reputational damage; loss of trust by data subjects.	1	2	G	NHSX - Joint Controller and Information Framework Agreement Staff contracts and mandatory training Processors - GDPR compliant DPAs in place Satisfactory completion of assurance checklist										
3	Adequate data processing agreements with relevant data processors;	Non-compliance with the data protection legislation; vulnerability of organisation against breach and possible regulatory action; loss of personal data to non-trusted sources; privacy risk to onward sharing of personal data; reputational damage; loss of trust by data subjects.	2	2	AG	AWS - AWS GDPR DATA PROCESSING ADDENDUM Microsoft - Microsoft Online Services Data Protection Addendum January 2020 Firebase - verify Pivotal - G-Cloud 11										
4	Lack of technical or organisational measures implemented to ensure appropriate security of the personal data	Non-compliance with the data protection legislation; vulnerability of organisation against breach and possible regulatory action; loss of personal data to non-trusted sources; privacy risk to onward sharing of personal data; reputational damage; loss of trust by data subjects.	1	2	G	Well estabished hosting arrangements testing in controlled environment										
5	Personal data not being encrypted both/either in transit or at rest	Non-compliance with the data protection legislation; vulnerability of organisation against breach and possible regulatory action; loss of personal data to non-trusted sources; privacy risk to onward sharing of personal data; reputational damage; loss of trust by data subjects.	1	2	G	Communication from mobile phone to the sonar backend is via HTTPS RESTful micro services over TLSv1.2 with other security protections. Via Firebase messaging service Packet data is encrypted with the reciving user's security key so only they can decrypt it Transmitted ID is encrypted Sonar ID and changes periodically										
6	Lack of testing which would assess and improve the effectiveness of such technical and organisational measures	Non-compliance with the data protection legislation; vulnerability of organisation against breach and possible regulatory action; loss of personal data to non-trusted sources; privacy risk to onward sharing of personal data; reputational damage; loss of trust by data subjects.	1	2	G	Pivotal test programme operating in a controlled environment.										
7	Inadequate or misleading transparency information	Non-compliance with DP legislation; reputational damage.	1	4	G	Privacy notice to be incorporated in App										
8	Misuse of reference code issued by app for test requests and results management	Risk that the code alone gives general public (non-key workers as set out by Gov policy) early access to testing? As it stands there is no way to verify the code is valid and I wouldn't want the app to be used to sidestep restrictions on testing. I'm not sure this question is in our direct scope but the testing centre needs to know the limits of this approach. I.e. anyone could be calling up and reciting any code. They should implement other checks to ensure those calling are eligible for a test. If this testing is restricted to IoW there is limited exposure but still it could open up an opportunity for anyone to get a test on the IoW, prompt people try visit IoW, sell their test etc.	3	1	AG	There is a checksum built into the code, so it is verifiable from a data integrity standpoint.										
9	Malicious access to Sonar backend by cyber attack Extraction and re-identification of Sonar backend data by combination with other data	Notifiable security breach. Breach of confidentiality. Reputational damage. Undermining purpros of app.	1	5	G	Technical security protections incorprated in system architecture.										
10	Idenification of infected individual due to minimal contact - e.g. isolated person with carer who is only contact	Identity of infected person implicitly revealed	3	1	AG	Risk understood and accepted by the Secretary of State										
11	Malicious or hypochondriac incorrect self diagnosis on app	Proximity users receive false proximity alerts	3	3	A	Adderssed in terms of use.										
12	Absence of controls over access to app by children	Inappropriate use by non-competent children resulting e.g. in false self-reported diagnosis and proximity alerts.	3	3	A	Requires system-wide response										
13	Lower than expected public trust at launch	Due to inaccurate reports (or high profile debate about the relative merits of a decentralised -v- centralised model) a suboptimal number of people download the app	2	3	AG	Extensive comms plan to public, and other stakeholders (inc civil liberties campaingers) to promote trust; publishing the Privacy Notice, DPIA and source code; leveraging the presence of and recommendations of the Ethics Advisory Board										
14	Uncertainty about whether users will be able to exercise SRRs in relation to data held in the Sonar backend	This will require users to have access to their Sonar ID. With this they may be able to make a request which will be processed via the NHS England and NHS Improvement SRR process. The technical practicality of this needs to be assessed. If users do not have access to the Sonar ID, SRRs may be exempt under Article 11. Users may uninstall the app from their phone at any time which will cause deletion of all the app data form the phone. This will not cascade to the Sonar backend. Exemption to right to erasure may be 17(1)(c) - overriding legitimate grounds - as the legal basis is 6(1)(e) not consent	1	4	G	There is no facility for users to access the Sonar ID in the Isle of Wight release. GDPR Article 11 provdes that "the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulatin" - e.g. respond to subjects' rights requests.										
15	Uncertainty over retention of individual data items	Whilst some of the data is useful on an ongoing basis for epidemiological research, other data items are not needed to be retained beyond their immediate use RSSI. Without a policy on this may be retained longer than necessary and breach GDPR Art. 5(e).	2	3	AG	In accordance with the law, personal data will not be kept for longer than is necessary. The exact retention period for data that may be processed relating to COVID-19 for public health reasons has yet to be set (owing to the uncertain nature of COVID-19 and the impact that it may have on the public). In light of this, we will ensure that the necessity to retain the data will be routinely reviewed by an independent authority (at least every 6 months). There will be a research value for data selected by the NHS COVID-19 App, along with any other COVID-19 data set. Whilst the NHS COVID-19 App will ensure that information processed within the NHS COVID-19 App cannot be identified, there may be requests to process data from the app for research purposes, which may be linked with identifiable data. All such requests will be subject to further approvals and independent oversight.										

Types of privacy risk

Risks to individuals

- Inadequate disclosure controls increase the likelihood 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 people's knowledge.
- New surveillance methods may be an unjustified 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 than individuals might 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 or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation 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 necessary.

Compliance risk

- 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.

Associated organisation/corporate risk

- 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 fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging 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 organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Risk guidance

Guidance for completing a risk register

What is the actual risk ? (really consider and evaluate what the risk is).
Is the risk clear and concise and articulated with appropriate use of language, suitable for the public domain.
All risks need to proceed with the wording: **There is a risk that …… would lead to …….**
'Risk owner' and 'Action owner' should include full job title (not names).
Acronyms must be spelt out in the first instance.
Be careful and sensitive about the wording of the risk, as **risk registers are subject to Freedom of Information (FOI) requests.**
Don't reference blame to other organisations in the risk register (the register may be made available in the public domain).
Does the risk belong to a business area within the NHS England or another NHS body, e.g. DH.
Risk assessment / scoring in line with the guidance (really ask yourself how likely the realisation of the risk is).

The risk register

Risk owner – the owner is responsible for the management and control of all aspects of the risk. Each national directorate has an assigned National Director who as Senior Responsible Owner (SRO) is the responsible risk owner for the strategic risks.
Risk description- a statement describing the cause, risk event and impact.

Mitigating actions - systems and processes that are in place and operating that mitigate this risk. This can include assurances: Internal assurance - internal evidence that this risk is being effectively managed (e.g. Board reporting, sub-committee and internal audit committee reviews), and external assurance - external evidence that this risk is being effectively managed (e.g. planned or received external audit reviews).

Action owners - all risks have an action owner to who has delegated responsibility for the on going control, monitoring and status reporting.
Completion date for actions - each mitigating action should have a completion date, for when the action will be completed.

Scoring the risks

NHS England risks should be scored between 1-5 for both likelihood and impact.
The table below provides descriptions of likelihood and impact scoring.

	Score				
Likelihood score	1	2	3	4	5
Descriptor	Rare	Unlikely	Possible	Likely	Almost Certain
Frequency - how often might it happen?	This probably will never happen/recur	Do not expect it to happen/recur, but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur, but is not a persisting issue or circumstance	Almost certain to happen/recur; possibly frequently

	Score				
Impact score	1	2	3	4	5
Descriptor	Very low	Low	Medium	High	Very high
Impact should it happen?	Unlikely to have any impact	May have an impact	Likely to have an impact	Highly probable it will have a significant impact	Will have a major impact

NHS England uses a RAG matrix rating system. RAG stands for red, amber, green. To achieve a RAG rating, each risk first needs a likelihood and impact score.

Each risk will be RAG rated by taking the likelihood and impact scores, and using the matrix below:

Impact						
	Very High -5	A	A/R	R	R	R
	High - 4	A	A	A/R	R	R
	Medium - 3	A/G	A	A	A/R	A/R
	Low - 2	G	A/G	A/G	A	A
	Very Low - 1	G	G	G	G	G
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
		Likelihood				

Using the risk "RAG" rating system for scoring risks means risks can be ranked so that the most severe are addressed first. Decisions can then be made as to what mitigating action can be taken to alleviate the risk.