### Privacy Impact Assessment - Risk Register

#### Initiative name: Covid-19 App (06/05/2020)

**Privacy Impact Assessment - Risk Register**

<table>
<thead>
<tr>
<th>Risk Reference</th>
<th>Risk Category</th>
<th>Likelihood</th>
<th>Impact</th>
<th>RAG Status</th>
<th>Responsibility</th>
<th>Status/Progress</th>
</tr>
</thead>
</table>
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.
- 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.

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

<table>
<thead>
<tr>
<th>Score</th>
<th>Impact score</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Descriptor</td>
<td>Very low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Very high</td>
<td></td>
</tr>
<tr>
<td>Impact should it happen?</td>
<td>Unlikely to have any impact</td>
<td>May have an impact</td>
<td>Likely to have an impact</td>
<td>Highly probable it will have a significant impact</td>
<td>Will have a major impact</td>
<td></td>
</tr>
</tbody>
</table>

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:

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.