This Data Protection Impact Assessment has been carried out to address the differences in the deployment of the NHS Test and Trace app in Wales. The full Data Protection Impact Assessment has been carried out by the Data Controller, the Department of Health and Social Care (DHSC) and the link to the full document can be found inside.

This Data Protection Impact Assessment must be read in conjunction with the full DHSC document.
Data Protection Impact Assessment

Introduction

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. Unfortunately, these issues are often bolted on as an after-thought or ignored altogether. Such concerns in this programme are managed through the completion of a Data Protection Impact Assessments (DPIA). Previously called Privacy Impact Assessments, since the implementation of the General Data Protection Regulation in May 2018 they are a legal requirement for all projects involving Personal Data / Personal Identifiable Information, where the processing is believed to present a high risk to data subjects.

Data Protection Impact Assessments

The Public Health Wales Data Protection Impact Assessment is a two stage process.

I.T. implications

It is essential that before any development work is carried out on any project which will have any IT implications, advice MUST be sought from the Head of IM&T by submitting a service point request.

The project lead must complete the following declaration prior to submitting the DPIA.

*I confirm that there are IT implications for this project

*I confirm that there are no IT implications for this project and no IT advice is required

*Delete where non-applicable

Signed: ___________________________ Data Protection Officer

Please note that DPIAs will not be accepted without the declaration signed
Cross references to other Data Protection Impact Assessments

Any other connected Data Protection Impact Assessments must be referenced here.

<table>
<thead>
<tr>
<th>Title</th>
<th>Responsible Organisation</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHSC Test Trace and Trace App</td>
<td>DHSC</td>
<td>Lee Cramp DHSC DPO</td>
</tr>
<tr>
<td>TTP Contract Tracing System v3</td>
<td>Public Health Wales</td>
<td>John Lawson</td>
</tr>
</tbody>
</table>


Data Protection Impact Assessment

Stage 1 – Brief, high level description of the project.

The Department of Health and Social Care (DHSC) have developed a mobile application (App) to contribute towards the response of the coronavirus outbreak. The App is part of the NHS Test, Trace and Protect programme which is overseen by the DHSC.

The DHSC have completed a full DPIA that can be found here: NHS COVID-19 app: DPIA

This DPIA addresses any differences in the use of the App in Wales.

Table 1 Data to be collected - see definition of identifiable, anonymised and pseudo anonymised below:

<table>
<thead>
<tr>
<th>Personal data (Table 1 below)</th>
<th>Tick (All that Apply)</th>
<th>Special Category data (Table 3 below)</th>
<th>Tick (All that Apply)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
<td>Racial / ethnic origin</td>
<td></td>
</tr>
<tr>
<td>Address (home or business)</td>
<td></td>
<td>Gender</td>
<td></td>
</tr>
<tr>
<td>Postcode</td>
<td></td>
<td>Political opinions</td>
<td></td>
</tr>
<tr>
<td>NHS No.</td>
<td></td>
<td>Religious beliefs</td>
<td></td>
</tr>
<tr>
<td>Telephone number</td>
<td></td>
<td>Trade union membership</td>
<td></td>
</tr>
<tr>
<td>Email address</td>
<td></td>
<td>Physical or mental health</td>
<td></td>
</tr>
<tr>
<td>Date of birth</td>
<td></td>
<td>Sexual life</td>
<td></td>
</tr>
<tr>
<td>Payroll number</td>
<td></td>
<td>Criminal offences</td>
<td></td>
</tr>
<tr>
<td>Driving Licence [shows date of birth and first part of surname]</td>
<td></td>
<td>Biometrics; DNA profile, fingerprints</td>
<td></td>
</tr>
<tr>
<td>Photo / video / voice recording / other image</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sensitive data (Table 2 below)

| Bank, financial or credit card details |                       |
| Mother's maiden name                  |                       |
| National Insurance number             |                       |
| Tax, benefit or pension Records       |                       |
| Health, adoption, employment, school, Social Services, housing records | | | |
| Child Protection                      |                       |
| Safeguarding Adults                   |                       | Any other data to be collected        |                       |
Comments

App users are asked to confirm they are over the eligible age to use the app.

No other personal data is collected (refer to DHSC DPIA)

- the postcode district you provide when you install the App
- the symptom information you enter onto the App
- the QR codes of the venues that you scan into the App
- the 2 types of codes described above, which are generated every day and every 15 minutes respectively for contact tracing purposes

Definitions:

Identifiable personal data:
Individuals can be identified in a number of different ways.

- direct identification, where someone is explicitly identifiable from a single data source, such as a list including full names;
- indirect identification, where two or more data sources need to be combined for identification to take place

An individual may be directly identified from their name, address, postcode, telephone number, photograph or image, or some other unique personal characteristic.

An individual may be indirectly identifiable when certain information is linked together with other sources of information, including, their place of work, job title, salary, their postcode or even the fact that they have a particular diagnosis or condition.

Anonymised data:

- Information which does not relate to an identified or identifiable natural person;
- personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable
Anonymisation is the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified.

*Pseudonymised data:*

Pseudonymization enhances privacy by replacing most identifying fields within a data record by one or more artificial identifiers, or pseudonyms. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field.

Specifically, the GDPR defines pseudonymization in Article 3, as “the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.” To pseudonymize a data set, the “additional information” must be “kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person.”

NB. If you intend to take identifiable data and anonymise it in order to undertake you work, this is not the same as using anonymous data. The act of data anonymization is data processing in itself and you must have the appropriate legal basis for it before you can start.

*Data Protection Impact Assessment Screening Questions. To be completed by the project lead*

For screening questions refer to master DHSC DPIA Test and Trace App: [NHS COVID-19 app: DPIA](#)
<table>
<thead>
<tr>
<th><strong>Decision</strong></th>
<th><strong>Rationale</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Full DPIA required</td>
<td>This DPIA refers in the main to the DHSC DPIA Test and Trace App, there are some small differences in Wales which are covered in this DPIA.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Completed by:</th>
<th>Signature: John Lawson</th>
<th>Date: 24/09/2020</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Data Protection Officer</th>
<th>Signature: John Lawson</th>
<th>Date: 24/09/2020</th>
</tr>
</thead>
</table>
Data Protection Impact Assessment

**Stage 2 – Full Data Protection Impact Assessment**

Section 1 – More detailed description of the project. Please provide Project Initiation Document or Business Case if available.

The NHS Test & Trace App (“app”) is a mobile phone application that is part of the NHS Test and Trace Service, which is designed to break the chains of transmission of COVID-19. By using the app, users will help to protect themselves and those around them – their friends, family, colleagues and local communities, and enable society to return to a more normal way of life. The app is a medical device providing maximum freedom at minimum risk.

The objectives of the app are to:

- create an enduring new medical technology to manage public health
- promote behaviour change by helping people manage their risk exposure
- identify and inform people to help communities manage health emergencies
- reduce disease transmission by giving users easy access to health services
- support and inform users during isolation

The behaviour sought by the app from users is to:

- download the app and use it daily
- keep the app ‘on’ and carry their phone at all times
- follow instructions issued by the app
- ‘pause’ the app when appropriate
- enter symptoms and take a test quickly when told to
- self-isolate (as we expect of everyone) if a user tests positive for COVID-19
Data Protection Impact Assessment

More information can be found in the master DHSC DPIA Test and Trace App: NHS COVID-19 app: DPIA

Note: in Wales where a user checks in to a venue by scanning a QR code, the QR code element (location logging) is to allow PHW to notify people who have been in high risk premises. The premises display the poster, and app users scan in and out. The app records that they have been there and when.

If a problem is found within the premises PHW can log this with the app and it pushes the risk message out to app users if they have recorded they were there at the appropriate time. It does not feedback to PHW who or how many devices actually displayed the message.

PHW have no access to the data, only to a database of premises that have signed up to get a QR code.

The app is not a replacement for the requirement to keep a log of anyone. The app only allows people to keep a list of where they have been as an aide memoir if contact traced, or to allow them to receive notifications if a higher number of cases have been associated with a venue.

An app user can choose not to scan in, and delete their attendance at the venue.

Section 2 – Description of the data / information to be collected and the legal basis for collection

The legal basis for processing is set out in the master DHSC DPIA Test and Trace App: NHS COVID-19 app: DPIA

Section 3 – Data flow diagram

(Use this section to sketch out the flow of data. Keep the description as simple as possible (e.g. Data inputs – Data processing by PHW – Internal data sharing – External data sharing). If necessary or convenient, attached the data flow diagram as a separate document)

The diagram below and the narrative explains the differences on how the testing process via an API in the Tracking App works within Wales
Each of the interactions made with the underlying solution architecture are expanded in this narrative accompanying the diagram. It’s important to note here that an underlying design principle set by NHS Digital is to separate the storage and use of the CTA Token from the wider patient record.

This is a security principle associated with the decentralised approach to the NHS App’s delivery. NHS Wales will therefore prevent the sending of the CTA Token into the Wales Laboratory Information Management System (WLIMS) and in turn into the wider electronic patient record made available for viewing in applications like the Welsh Clinical Portal (WCP). It will however store the CTA Token temporarily in the National Architecture’s State Engine, and against the WLIMS Episode Number (i.e. the number used to generate the test order in WLIMS via the ETR). This enables the retrieval of the CTA Token at appropriate points in the process (i.e. immediately prior to a text message to the citizen being created or when a result is sent back to the NHS Digital Platform for reconciliation with the citizen in the App).
Data Protection Impact Assessment

Section 4 – Use of third party data processors

The DHSC are the data controllers for the test and trace app. Details of the data processors can be found in the master DPIA Test and Trace App: NHS COVID-19 app: DPIA

Section 5 – Consultation proposals

(Use this section to describe what consultations have been undertaken or are proposed)

This process has been developed by DHSC in consultation with; TTP Programme Board/Welsh Government, and the Local Authorities and Local Health Boards/Trusts.

Section 6 – Initial Risk Assessment

Use this section to describe the risks. In this context you are describing the risks either to the rights and freedoms of the data subjects, or the risks to Data Controllers from non-compliance with the requirements of Data Protection legislation. Certain generic risks have also been identified, which should be assessed accordingly. All risks have been identified and recorded on a separate risk register according to Public Health Wales’ procedure, which is attached.

Refer to risk assessment in the master DPIA Test and Trace App: NHS COVID-19 app: DPIA

Section 7 – Complaints and management of the rights of data subjects

All issues around the management of the rights of Data Subjects and complaints about the data processing will be directed to the Data Controller as per their Privacy Notice.

Refer to DHSC Test and Trace App privacy notice NHS COVID-19 app: privacy notice
Section 8 - Linking the DPIA to the data protection principles

The General Data Protection Regulations (GDPR) 2018 contains 6 principles for Data Protection with which all controllers are expected to demonstrate compliance. By answering these questions during the DPIA process you will identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Refer to DHSC Test and Trace App privacy notice: [NHS COVID-19 app: privacy notice](#)