A3C Management
SAFETY | QUALITY | ENGINEERING

The predictable should never be a surprise

CONTACT TRACING FOR COVID-19

CURRENT POSITION

There are regulations in place for certain industry sectors to ensure that they have track and trace controls in place. This specifically relates to venues in hospitality, the tourism and leisure industry, close contact services and local authority facilities.

All of these organisations must:

- Every member of every party of customers or visitors (up to 6 people) to provide their name and contact details.
- Keep a record of all staff working on their premises and shift times on a given day and their contact details.
- Keep these records of customers, visitors and staff for 21 days and provide data to NHS Test and Trace if requested.
- Display an official NHS QR code poster from 24 September 2020, so that customers and visitors can 'check in' using this option as an alternative to providing their contact details.
- Adhere to General Data Protection Regulations (GDPR).

Hospitality venues must also refuse entry to those who refuse to participate. Failure to do any of these requirements will result in fixed penalty fines.
After months of setbacks, a contact tracing app was rolled out from the 24 September 2020, which uses Bluetooth technology to track time and distance between smartphone devices.

The Government has urged businesses to display NHS QR Code posters on entry to their premises, which are able to be scanned by the app, so that individuals that attend certain locations can be identified and notified in the event of an outbreak related to that location. The app will then be used in conjunction with the more traditional approach to contact track and tracing methods, by staff employed to manually carry out these duties.

The contact tracing information remains on the individual's phone for 21 days before being deleted, which should be sufcient time for individuals to be contacted in time to isolate and mitigate further risks to themselves or those around them.

The track and tracing app has been jointly developed with Google and Apple following the abandonment of the government's original application development, due to privacy risks associated with storing large volumes of personal data on a central database. This new app only sends data between devices when Covid-19 is detected, and it is hailed as being more in line with privacy requirements.

The ICO have released a statement supporting the use of the app and their commitment to offer guidance during the lifecycle of the application, up to and including decommissioning, stating:

"We will continue to offer that guidance during the life of the app as it is further developed, rolled out more widely and when it is no longer needed. This includes an audit of the app and ensuring that it is properly decommissioned."

The Government has urged businesses to display NHS QR Code posters on entry to their premises

They have also released a comprehensive guidance document that needs to be followed as part of the development, Contact Tracing — Data Protection Expectations on App Development.

In addition to the app, organisations will be expected to have their own track and trace mechanisms in place, which must also consider risks to Data Subjects relating to the type and volume of personal data gathered and the level of security and privacy built into the Track and Trace mechanisms adopted by an organisation.

Legal Requirements

In July 2020 the Health Protection (Coronavirus, Restrictions) (England) Regulations 2020 came into force, which defines new legislation to address 'the serious and imminent threat to public health' caused by the Coronavirus Pandemic. Organisations should consult Section 2 of this legislation which states industry specific restrictions relating to Covid controls.

This legislation is constantly changing as the Covid situation evolves and so this legislation should be consulted in conjunction with the subsequent amendments. The Regulations address points like the changing local lockdown restrictions or changing national lockdown measures. Links to the most up to date legislation and amendments can be found at the on the Barbour Service.

On the 17 September 2020, the Health Protection (Coronavirus, Collection of Contact Details etc. and Related Requirements) Regulations 2020 were introduced to support the new track and trace requirements for organisations.

As part of these regulations, there are a number of mandatory requirements that organisations need to be aware of when considering the use of track and trace controls. These requirements are also set out in the Government guidance relating to NHS Test and Trace Service in the Workplace.

These requirements include:

- Asking every member of every party of customers or visitors (up to 6 people) to provide their name and contact details. Where the party is larger than 6, then it must be broken down into smaller groups and have a designated person provide their details.
- Details gathered from the individuals must be:
  - their name
  - the time that they visited the venue
  - if they are part of a group, the size of group
  - either their email address, phone number or postal address
- Keeping a record of all staff working on their premises and shift times on a given day and their contact details.
- Keeping these records of customers, visitors and staff for 21 days and provide data to NHS Test and Trace if requested. Following which they must be securely destroyed as soon as possible after that date.
- Displaying an offcial NHS QR code poster from 24 September 2020, so that customers and visitors can 'check in' using this option as an alternative to providing their contact details.
- Adhering to General Data Protection Regulations (GDPR).

Failure to comply with requirements to gather tracking information can result in fixed penalty fines that range from £500 for the first infringement, up to £4,000 when multiple infringements are identified.

These requirements apply to specific industry sectors, however they may be adopted by other organisations that identify a risk that would necessitate these kinds of controls to be in place. As part of developing and establishing these controls, organisations must also consider how any bespoke controls they develop conform to the requirements of GDPR and the Data Protection Act 2018.

This would include conducting a Data Protection Impact Assessment (DPIA) to fully understand the impact of their system upon an individual's rights and freedoms. A DPIA is a process to help you identify and minimise the data protection risks of a project. This DPIA should consider:

- privacy as part of development process for the track and trace systems
- data gathering requirements
- secure storage
- retention periods

The Assessment should ensure that the amount of data gathered is limited only to what is necessary and that processing activities are limited only to those necessary for carrying out Track and Trace activities.

Note that the Government failed to meet the legal requirement to conduct a DPIA for the initial launch of the Track and Trace App, however this should not be seen as an endorsement for not conducting DPIA's within organisations that need to implement a Contact Tracing system.

Any organisation implementing a Contract Tracing system should conduct a DPIA either using their own DPIA process or with reference to the DPIA guidance released by the ICO. The ICO guidance includes several screening checklists to help with the process.

INFORMATION
Organisational Track and Trace Mechanisms

To comply with legal requirements, some organisations (see above) will be required to adopt their own systems to support contact tracing in the event of a Covid-19 outbreak associated with their venue.

As previously mentioned, these systems will need to be carefully designed and implemented in order to comply with Data Protection regulations.

To assist in developing a compliant system, the ICO has published guidance based on an **'ABCDE'** acronym, which relates to the following steps:

Ask for only what is needed

Only ask people for the specific information that has been set out in government guidance. This may include things like their name, contact details and time of arrival.

Be transparent with customers

Be clear, open and honest with people about what you are doing with their personal information. Tell them why you need it and what you'll do with it. This could be done by displaying a notice in your premises or by including it on your website.

Carefully store the data

Keep personal data collected secure on a device if you're collecting the records digitally or, for paper records, keeping the information locked away and out of public sight.

Don't use it for other purposes

The personal information that you collect for contact tracing cannot be used for other purposes, such as direct marketing, profiling or data analytics.

Erase it in line with Government guidance

Do not keep the personal data for longer than the government guidelines specify. It's important that you dispose of the data securely to reduce the risk of someone else accessing it. For example, shred paper documents and permanently delete digital files from your recycle bin or back-up cloud storage.

This information can be found at 'Contact tracing - protecting customer and visitor details' on the ICO website, and is further supported by their guidance 'Collecting customer and visitor details for contact tracing.' Key points that you should be aware of in adhering to Data Protection Legislation (GDPR and the Data Protection Act 2018) are as follows:

Data Limitation - you must ensure that the data you gather is the least amount possible to fulfil the purpose for which it is required, in this instance contact tracing. If you decide to gather more than a name and contact details then you should consider why you believe you need this.

Data Protection Notices - you must provide individuals with information that explains what data you are gathering, why you are collecting it, how it will be used, who it will be shared with and how long you will keep it. These notices should be in simple language, relative to the people you will be dealing with.

Lawful grounds - the lawful ground for gathering contact tracing information is currently a legal requirement. However, should you gather more information than is needed to meet this legislation, or if you were to use it for any other reason than track and trace, you will need to provide appropriate notices and establish what lawful grounds you are gathering and processing this data under.

Retention periods - the track and trace app currently stores individuals' information for 21 days before deleting it. If you were to keep data for any longer than this, then you should have clear reasons for this extended duration, directly related to track and trace reasons.

Accuracy of Information - under track and trace it is only necessary to keep an accurate record of the information provided, and you would only need to ask for clarifi cation of this if you strongly believed that the information was incorrect. There is no requirement to ask for evidence such as driving licenses, passports, etc.

Individuals' Rights - an individual has the right to ask you to tell them what information you have on them, and to request that it is corrected if the information is found to be incorrect.

Sharing of Information - you should only share contact tracing information with public authorities, and should ensure that you verify the identity of anyone requesting this information on behalf of a public authority.

Handling of Information - you should restrict access to tracking information to a limited number of staff, and train them regarding the need to keep this information private and secure. Your staff should be aware of the potential security risks.

As of the 24 September 2020, organisations that are required to have contact tracing systems in place, must also display the Government poster showing the QR Code for 'checking in' with the Governments contact tracing app. The details of how this app works is documented below.

Data Protection Impact Assessments

Conducting DPIA's is a good way to really under-stand the importance of protecting track and trace information and informing an organisation on data handling and staff training requirements.

When conducting Data Protection Impact Assessment (DPIA), you are considering risks and impacts to individuals and not risks and impacts to your business. These impacts include the risk of physical or material damage to an individual psychological harm such as emotional distress, anger, embarrassment, etc that could negatively impact upon their state of mind.

For contact tracing you should consider that individuals not only want to keep their contact information safe, but

Keep personal data collected secure on a device if you're collecting the records digitally or, for paper records, keeping the information locked away and out of public sight

also the potential risks of this information being disclosed. The types of risks you should consider include scam communications from bad actors claiming to be track and trace agents or other types of social engineering attacks designed to defraud and individual.

Other issues relating to the inappropriate use of track and trace data could be embarrassment or distress to individuals if health conditions, such as Covid infection, became public knowledge rather than privately communicated through official government channels.
Data Protection Security Risks Management

Contact tracing systems may range from simple paper records containing individuals' details, to com-puterised systems. Whatever the system is, careful attention will need to be paid to how this information is stored and secured, and who has access to this information.

To protect this information an organisation should consider:

Unauthorised Access

- Access controls for computerised systems, with a formal process for authorising users who have access to these systems.
- Strong password enforcement for systems containing personal data.
- Encryption of electronic data where possible.
- Physical access controls for hard copy information, including a register of authorised key holders for rooms, cupboards and cabinets containing personal data.

Availability of Information

Backup processes for digital information should be considered to ensure that important data is not lost due to device failure or human error.

Data Protection Requirements

- Formal processes should be in place to ensure that retention periods are strictly observed and that there is a formal process in place for the secure deletion of data that exceeds retention periods.
- Confidentiality Agreements for all staff who have access to personal data.
- Good policies on the handling of personal data by staff , with training to support the communication of policies and processes designed to protect personal data. This should include restrictions on sharing or communicating personal data without authorisation.

Welsh Data Breach exposes Information of Covid-19 Patients

While this case is not in relation to contact tracing information, it serves as reminder that data breaches can happen. Public Health Wales confirmed a data breach which involved the personally identifiable data of Welsh residents who had tested positive for Covid-19.

The incident, which was the result of individual human error, occurred when the personal data of 18,105 Welsh residents who had tested positive for Covid-19 was uploaded by mistake to a public server where it was searchable by anyone using the site.

After being alerted to the breach, Public Health Wales said the data was removed the next morning.

In the 20 hours it was online it had been viewed 56 times.

The risk of identification for these individuals therefore was higher but still considered low, Public Health Wales said. An external investigation into the full circumstances surrounding the data breach and any lessons to be learned has been commissioned [at time of writing].

Data Protection Controls - the use of Children's data.
Where possible, gathering children's personal details should be avoided. In family groups it is advisable only to gather information regarding adults.

In instances where the group consists of only children, such as visiting a café or leisure venue, then you should follow guidance from local government regarding any age restrictions on gathering personal data. Where this

guidance doesn't exist, you should evaluate whether the individual is competent enough to understand what they are agreeing to, if this is not clear then you should not gather their information.

Bear in mind that if you are gathering information from a younger individual, your Privacy and Consent notices should be written in a way that someone from that age group can clearly understand.

In all cases, you should consider the potential risks to children's data to be greater than to adults so you must make sure that you handle it particularly carefully.

Test and Trace for Staff

All organisations must be operating a Covid safe environment, with appropriate social distancing controls and PPE in place. If this is being properly controlled then the likelihood that an infected member of staff has infected others around them at work, is quite low.

Staff exhibiting symptoms must therefore isolate in line with Government guidance and seek a test at the earliest possible time.

For staff that test positive, they will be contacted by the NHS test and trace and asked to provide details regarding anyone they have had close contact with. The follow-up from the NHS Test and Trace will then dictate the level of contact tracing that needs to take place following their investigation. Government guidance sets out what to do if you or someone you employ is contacted by NHS Test and Trace, including information about self-isolation and financial support.

For some organisations it may be advisable to have a policy which asks employees to tell their manager or HR if they experience Coronavirus symptoms. This may help them to manage any potential outbreak in the workplace, for example by establishing at an early stage who the employee has been in contact with at work and seeking to keep those individuals separate from others at work, if possible, or otherwise, potentially, away from the workplace.

ICO guidance on data protection and Coronavirus recommends that staff should be kept informed about possible cases of the virus amongst their colleagues, but individuals who have or may have the virus should not be named. You should only tell colleagues who have been in contact with the potentially infected person, and not the workforce more widely.

In some cases, it may be that employees are able to work out who the affected employee is, particularly if they have been split into small groups to work. In most cases, the duty to protect the health and safety of your employees by informing them that they may have been in contact with the virus will over-ride the confidentiality risk, but each situation should be considered individually.

The Government Track and Trace App Functionality

The new Test and Trace app works alongside traditional contact tracing and testing services and reflects current government policy on how the UK is dealing with the pandemic. This version is more than just a digital contact tracing app, with six functions at its core:

Location check-in: The app will let users securely (locally on their device) track the restaurants, bars, and other venues they have visited over the last two weeks by scanning QR codes at participating venues. This allows the app to alert you if one of these locations was judged to be high risk when you were there. This is driven by data from the Joint Biosecurity Centre (JBC) and local Health Protection Teams within a region.

Regional risk score alerts: The app will let users know the level of risk in their declared postcode district and notify people when it changes — this is driven by data from the Joint Biosecurity Centre and is one reason you're asked for your postal district.

Digital contact tracing: As before, the app notifies people who may have been in risky contact with someone who tested positive for Covid-19 and provides advice on what to do, including helping them book a free test. This

is now based on the ENAPI and is integrated with the clinical virology testing service so that only a valid test result can trigger notifications.

Symptom recorder: The app will let users record symptoms, point users to book a test if appropriate and access the latest medical advice and guidance.

Testing services: The app will let users order a test and get the results back through the app in a privacy-preserving way. In the future, users should be able to get their results in the app regardless of how a test is ordered, but that is not in this current (September) release.

Self-isolation countdown and advice: The app will let you know how long you need to continue to self-isolate and what you can do to keep yourself and others safe.
This is the first release's functionality; the app will evolve as the UK response does, so it must be extensible. New functionality is designed with security at its core.
These functions and the development of the technology behind them has been reviewed by the National Cyber Security Centre (NCSC) to ensure that the app is safe and secure to use, that the privacy of individuals is maintained and the use of personal data was communicated to them in a transparent manner. More details can be found on the NCSC website.
Information provided by venue's and the Contact Tracing App are then used by the NHS to identify and contact individuals who have been potentially exposed to the virus and they will be asked to isolate in line with government guidelines.

The NHS Test and Trace Methodology

Individuals will be contacted by email, text or phone.
Text messages will come from NHS tracing. Calls will come from 0300 0135000.

Children under 18 will be contacted by phone where ever possible and asked for their parent or guardian's permission to continue the call.

What People will be Asked to do:
Individuals will be asked to sign into the NHS Test and Trace contact tracing website at https://contact-tracing.phe.gov.uk.

On the contact tracing website, they will be asked for information including:

- name, date of birth and postcode
- if they live with other people
- any places they've been to recently, such as a workplace or school
- names and contact details of any people they were in close contact with in the 48 hours before symptoms started (if these details are known).

If they cannot use the contact tracing website, they will be asked for this information over the phone.

On 8 October 2020, the government's guidance on how NHS Test and Trace works was updated to stress that the requirement to self-isolate if you test positive or are contacted by NHS Test and Trace and asked to self-isolate has changed from guidance to law.

NHS Test and Trace: Privacy Information

The Department of Health and Social Care (DHSC) has released a privacy notice, which sets out information

Where possible, gathering children's personal details should be avoided

on how personal data is collected, used, shared, stored, and disposed of in the provision of the NHS Test and Trace programme. The DHSC is the 'data controller' for personal data processed within the three main parts of Test and Trace service, namely: test, trace and contain (which relates to working with local authorities to identify outbreaks and to take coordinated action to contain them). The full privacy notice can be found here. A summary of the notice is also available here.

Contact Tracing Figures

According to GOV.UK, more than 550,000 contacts were reached by NHS Test and Trace and told to isolate in the week before Christmas 2020. From 17 to 23 December, 181,910 people who tested positive were successfully reached. This was 58,398 more than the previous week. In addition, it notes that cases are being reached more quickly, with 80.2% reached within 24 hours, compared with 77.1% the previous week.

Reasons for these improvements are suggested as improv-ing the contact tracing website, introducing more effective systems for contacting members of the same household and increasing the number of local authority tracing partnerships.

Due to the emergence of a more transmissible strain of coronavirus, the service has prioritised creating a more robust contact tracing system, as well as making more tests available.

In aiding the national contact tracing system, the government commented that the NHS COVID-19 app became the second most downloaded free iPhone app on its app store in the UK in 2020.

And as of 23 December, the NHS COVID-19 app in England and Wales had been downloaded 20.9 million times.

KEY ACTIONS

The following steps are the basic steps that organisations need to take in order to understand how Contact Tracing affects their organisation, and whether it falls under the government criteria for mandatory contract tracing mechanisms.

If your organisation is required to implement contact tracing then:

Develop and implement a contact tracing methodology which includes:

1. Every member of every party of customers or visitors (up to 6 people) to provide their name and contact details.

   - keep a record of all staff working on their premises and shift times on a given day and their contact details
   - keep these records of customers, visitors and staff for 21 days and provide data to NHS Test and Trace if requested
   - display an official NHS QR code poster from 24 September 2020, so that customers and visitors can 'check in' using this option as an alternative to providing their contact details
   - adhere to General Data Protection Regulations

2. Conduct a DPIA and follow the ICO 'ABCDE' Guidance for developing a contact tracing system and ensure that any high risks to individuals have been mitigated prior to implementation. If there are high risks that cannot be mitigated, contact the ICO for advice.

3. Create and prominently display very clear information for individuals leaving their details, the reasons for gathering information about them, how it will be used and how long it will be maintained. (Refer to the ICO's 'Make your own privacy notice').

4. Ensure that all data gathered is securely stored (these requirements should come from the DPIA).

5. Ensure that a mechanism is in place to manage retention periods, so that personal data is not held for any longer than necessary.

6. Obtain and display the Government Test and Trace QR Code poster.

7. Train your staff to understand the importance of gathering and protecting personal data, especially sensitive data that relates to an individual's health, family, friends and living arrangements.

RELATED DOCUMENTS AND FURTHER INFORMATION

Department of Health and Social Care:

- Maintaining Records of Staff, Customers and Visitors to Support NHS Test and Trace
- NHS Test and Trace: How it Works
- Test and Trace - Overarching Privacy Notice
- Test and Trace - Overarching Privary Notice

Information Commissioner's Office

- Collecting Customer and Visitor Details for Contact Tracing
- Contact Tracing - Data Protection Expectations on App Development
- Data Protection and Contact Tracing - Five Steps for Businesses
- Data Protection Impact Assessments (DPIAs), Accountability and Governance - General Data Protection Regulation
- Make your own Privacy Notice
- Processing Children's Data

Legislation

- Coronavirus Act 2020
- Health Protection (Coronavirus, Collection of Contact Details etc and Related Requirements) Regulations 2020

National Cyber Security Centre

- NHS Test and Trace App Security Redux