Public Health Agency

DATA PROTECTION IMPACT ASSESSMENT TEMPLATE REPORT

DPIA Ref no. *(Information Governance to provide)*	
DPIA 03/20	
Project Name	
PHA Contact Tracing Service and Contact Tracing Information System	
Business Area	
PHA Health Protection	
Information Asset Owner	Project Manager
Dr Gerry Waldron	**Jennifer Lamont**

Contents

Common acronyms	
TTP	Test Trace and Protect
CTS	Contact Tracing Service
CTIS	Contact Tracing Information System

CTR	Central Test Registry
DST	Digital Self Trace

DPIA Contact Tracing Service and Contact Tracing Information System

1. Need

Contact tracing is a central tenet of the DoH “Test, Trace, Protect” strategy which outlines the measures to control the prevalence of COVID-19 in Northern Ireland.

Contact tracing involves the processing of personal data in order to identify and communicate with the close contacts of confirmed cases. The overall purpose of contact tracing is to break chains (and potential chains) of infection by advising people who are at risk of contracting or have contracted COVID-19 to self- isolate for the incubation period of the disease to avoid passing on the infection to others.

Contact tracing has been part of the core business of the PHA since its inception and is used in the management of various communicable diseases such as meningitis and measles as well as outbreaks of food poisoning. This COVID-19-specific Contact Tracing Service (CTS) differs in its scale and duration. A new dedicated IT system has been developed to support the service during these un-preceded times.

This DPIA covers the core ‘manual’ COVID 19 Contact Tracing Service operated by the Public Health Agency (PHA), and associated Digital Self-Trace platform and analytics platform, as described below. A DPIA is required because personal and special category (health) data is collected, used and stored as part of the service. This is described throughout this assessment. The PHA is the data controller for the personal data used in the Contact Tracing Service.

A DPIA is required as the PHA CTS involves the collection, storage and processing of personal and special category (health) data of confirmed cases and their contacts.
The personal data is used for the following purposes:

- To contact the confirmed case, to provide public health advice if appropriate and to seek information on others that they have been in contact with;
- To contact those who have been in contact with someone who has tested positive, to give appropriate public health advice to self-isolate and seek a test if symptomatic, in order to prevent further transmission of the virus; and
- To identify and manage clusters of disease.

Data is also used for public health surveillance, identifying trends in the COVID 19 outbreak and to prevent/control spread.

Disease surveillance is a core public health function, using data in a timely manner, to inform decisions and actions across the public health system to help control the spread of disease. Surveillance involves gathering a wide range of data about a disease from a range of sources, to provide situational awareness. This will include understanding the areas of the country which are most affected, whether symptoms are getting more severe and when the outbreak might have peaked. This will include combining, matching and comparing data from a range of sources to ensure a comprehensive picture and understanding of the disease and its impact. This is then used to inform public health action to help prevent and control the disease.

Surveillance also provides data to be used by modeller's, i.e. scientists who aim to predict how outbreaks will progress based on a range of different scenarios.

A separate, but connected, Analytic Platform is being utilised and its functionality and data flows will be included in this DPIA. Construction of the analytics platform has taken account of the risks and potential risks relating to the use of personal data as well as the necessity of using the data for surveillance purposes to inform decisions on measures to control and reduce the spread of COVID 19. This is described in the following sections of this DPIA. This will be aligned with and sit alongside assessment of the Contact Tracing Service, Contact Tracing Information System and Digital Self-Trace Platform.

Some personal data may be shared with third parties including public health bodies in England, Scotland, Wales and Republic of Ireland for the purposes of disease management in cases where a confirmed case or a contact has travelled between jurisdictions (See section 5.3).

Anonymised data may be shared through the HSC Data Warehouse for the purposes of research.

2. Purpose

Testing and contact tracing is seen as a cornerstone of strategies employed by countries to contain the spread of the coronavirus and save lives across the globe. On the 12th May 2020 the NI Executive published the document, 'CORONAVIRUS; EXECUTIVE APPROACH TO DECISION-MAKING' outlining a 'pathway to recovery' and stating "*As context to its reviews, the Executive will take account of measures to reduce transmission, including the increased availability of testing, the use of surveillance or tracking methodology and contact tracing for those who test positive for Coronavirus or who meet an appropriate clinical case definition. Where IT solutions, such as Apps, can assist, we will use them and encourage you to do the same. However, no matter how good such Apps are, they will have limited value unless used widely across society*." [1].

The PHA COVID 19 Contact Tracing Service is one part of a wider NI COVID 19 Test, Trace and Protect Programme (TTP). There are three discrete but linked elements in the delivery model for the overall TTP programme:

1. A digital, largely self-contained, suite of products that align with each other – the symptom checker app (live), the StopCOVIDNI (proximity) app (launched July 2020), an online test booking platform (part of the UK National Testing Initiative) and digital self-trace portal (launching October 2020).

2. A call centre – essentially operating as a proxy for those citizens who cannot or do not wish to use the digital products. Call handlers will have back office access to the digital platforms and will provide information on various aspects of the service.

3. The COVID 19 Contact Tracing Service, operated by the PHA - The CTS operates on two levels depending on the complexity of the contacts:
    - Trained contact tracers for the majority of cases; and
    - Health Protection Consultants (doctors with training in public health) for those cases where contacts or circumstances are complex.

    Contact Tracing is supported by an analytics platform. Allowing live analysis of COVID 19 case numbers as they are reported, enabling more accurate cluster tracing and analysis.

[1] https://www.executiveoffice-ni.gov.uk/publications/coronavirus-executive-approach-decision-making

This DPIA relates to the PHA CTS (including Digital Self Trace) and supporting analytic platform. The other elements will have separate DPIAs, prepared by the relevant data controllers. Further detail on the operation of the CTS is contained in the body of this DPIA.

There are two dedicated electronic information systems to support the contact tracing process:

1. Contact Tracing Information System (CTIS) has been developed to help support the manual contact tracing process.
2. Digital Self Trace (DST) has been developed to help support the electronic collection of contacts from a positive case to support the contact tracing process.

Contact tracing is an established method to help prevent the further spread of infections such as COVID-19. If we know who the contacts of COVID-19 cases are it makes it possible to quickly find other people who may have become infected and we can then stop any further spread of the infection.

Contact tracing works by identifying a confirmed case and asking them who they have been in contact with. Individual contacts are identified as being high risk, low risk or no risk. To be considered high risk you will have to have been in close contact with a confirmed case and have spent more than 15 minutes with them without any personal protection. This means that those who have casually passed by someone on the street will not be considered high risk.

The person with a confirmed infection, and their 'high risk' contacts will be given advice on what to do about managing symptoms and of the need to self-isolate to prevent any wider spread of the virus. They will be asked to identify their close contacts, during the period when they were infectious.

The identification of close contacts will either be:

- collected during the phone call with the CTS;
- by the individual with a confirmed case entering the information electronically via Digital Self Trace (DST)

Once all the data collection has been successfully completed the PHA CTS will close the data collection for the positive case and trigger an automated process sending all contacts, for that case, a SMS message. The SMS is addressed to the individual (using name supplied by positive case) and states that they are a close contact and need to self-isolate. In addition the contact tracers may then telephone these contacts, to provide advice on what they should do, including advice on self-isolation and testing.

The TTP programme is supported by the analytics platform. The information from COVID virus testing and contact tracing is hosted in a single secure environment which can be analysed, as required, to inform an appropriate response to this pandemic. Analysis of data is performed by PHA staff, with support from the Health and Social Care Board (HSCB) Digital Health and Care (DHCNI) team;

> The PHA Director of Public Health, Prof Hugo Van Woerden is the senior responsible officer for the analytics process.
>
> Technical support is provided by the HSCB including DHCNI team.

The PHA, as lead agency for the implementation of the DoH TTP Strategy, needs access to analysis of real-time data on positive cases and contacts in order to manage clusters (person, place and time) and take targeted actions to reduce the further spread of the virus. The new technical solution has been constructed to allow maximum utilisation and reuse of pertinent data.

3. Roles and Responsibilities

The PHA is the data controller for the personal data used in the Contact Tracing Service including the Contact Tracing Information System, as it is determining the means and purposes of the processing.

The PHA is responsible, along with its Data Processors and Sub-Processors, for the development, testing, security, operation and maintenance of the CTIS.

3.1 Governance

The contact tracing service sits within the governance structures of the PHA (the Agency Management Team and the PHA Board), and to the DoH via the Contact Tracing Steering Group (chaired by Dr L Mitchell, an independent chair appointed by the Chief Medical Officer) and the DoH Test Trace and Protect Oversight Board (chaired by Dr M McBride the Chief Medical Officer).

The Analytics Platform, and those operating the system, is overseen and directed by Prof Hugo Van Woerden, Director of Public Health for the PHA. Prof Van Woerden is also the Personal Data Guardian for the PHA.

There are a number of data processors and other roles that are assisting the PHA in designing, building and operating the Contact Tracing System (including Digital Self Trace and Analytics Platform), these are listed in Appendix A.

4. Processing Overview

This section of the document describes the data that will be processed, how much data is being collected and used, how often it will be processed, how long it will be retained for, and who the data relates to.

4.1 Context

The data is being collected in line with the UK and Northern Ireland's arrangements to respond to the COVID 19 pandemic. These arrangements are also in line with international measures to respond to COVID 19, as articulated by the WHO, including arrangements in the RoI (of particular relevance due to the land border, and the amount of cross-border movement). The establishment of contact tracing has been announced publically by the Minister of Health (NI) and subsequent press releases (https://www.health-ni.gov.uk/news/minister-sets-out-scale-contact-tracing-operation), providing public awareness around the purpose and need for this programme. A Test, Trace and Protect publicity campaign has been released: https://www.publichealth.hscni.net/COVID-19-coronavirus/testing-and-tracing-COVID-19 and information published.

The source data will come in the main from the Central Test Registry (schema in Appendix B). All citizens in NI with symptoms of COVID19 are entitled to a test.
Further information on the National Testing Programme and Privacy Notice relating to it can be found at: https://www.publichealth.hscni.net/COVID-19-coronavirus/testing-and-tracing-COVID-19/testing-COVID-19
A Privacy Notice relating to the PHA CTS can be found at https://www.publichealth.hscni.net/COVID-19-coronavirus/testing-and-tracing-COVID-19/privacy-information

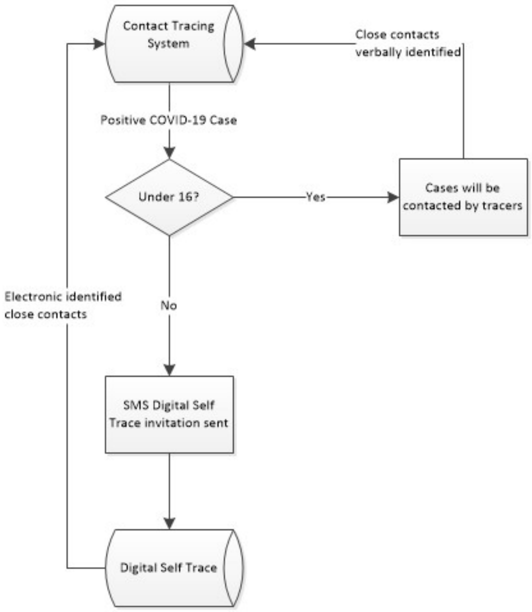
Testing via NI HSC laboratories is in line with routine normal Trust business.

Data will also be collected from the individuals who have tested positive (or their proxies if under age 16 years or without capacity) on the individuals they have been in contact with during the period of being infectious. The data collected on all contacts will be the minimum necessary to allow these people to be contacted (or where the contact is a child or a vulnerable adult, their representative or proxy).

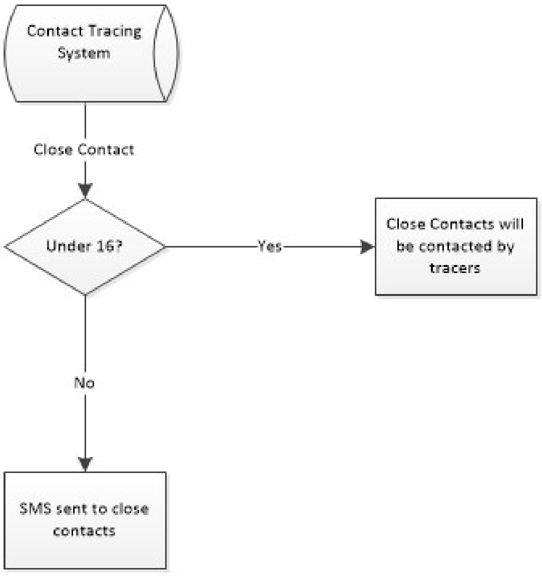
Adults and Children
As people of all ages – adults and children – can become infected with COVID 19 and test positive or be a contact of someone who has tested positive, the Contact Tracing Service will hold data on both adults and children.

Specific arrangements are in place in respect of children and vulnerable adults. If the confirmed case is under 16 or a vulnerable adult, the contact tracer will ask to speak to a 'proxy' (in the case of children, this would be their parent or legal guardian). If the contact tracer starts a call and during it, they feel that there is a capacity issue, they will refer to the contact tracing service clinical lead, who will undertake a competence test. While the scripts and data collection are the same as for other adults, the contact tracer, with their professional competence, would alter their approach depending on the situation and can also request additional support from the clinical lead.

If a child under 16 is identified as a close contact verbally, the contact tracer will ask for the parent/guardian's contact details from the confirmed case. However if this information cannot be provided, the contact tracer will call the child and ask to speak to their parent or guardian. If a child under 16 identified as a close contact via DST (based on response to question asking if the close contact is under 16) a close contact text message will not be sent and a tracer will make contact.


Contact Tracing System
Close contacts verbally identified
Positive COVID-19 Case
Under 16?
Yes
Cases will be contacted by tracers
Electronic identified close contacts
No
SMS Digital Self Trace invitation sent
Digital Self Trace

Digital Self Trace invitation SMS message will only be sent to over 16's, this is based on the DOB included in data that CTIS receives from the central test registry. The SMS message contains a test code, 2 by 3 alpha numeric blocks, without a valid test code the screens cannot be accessed nor data submitted.


Contact Tracing System
Close Contact
Under 16?
Yes
Close Contacts will be contacted by tracers
No
SMS sent to close contacts

Use of Data

The data will be held for the primary purposes of tracing and communicating with individuals who have been in contact with someone who has tested positive for COVID 19, to give them appropriate advice to help reduce/prevent the further transmission of the virus, and for management of clusters. Identifiable data is also required for cluster or outbreak management by health protection specialist staff, so that appropriate risk assessment and outbreak control measures can be implemented that is specific to the situation.

To enable the necessary linkages to be made the Analytics Platform requires the holding of full personal details regarding citizen identification. This is necessary to ensure that we have as much information as possible to augment the manual contact tracing system and to understand the patterns of transmission so that they may be successfully interrupted. This information is critical to the Public Health response and represents the quickest way to locally adjust guidance, reduce COVID 19 spread and save lives.

The analytics platform has become the quickest and most effective way of identifying local area involvement and therefore allowing rapid targeted responses. Test Track Protect data enters the Analytics Platform via the Contact Tracing Information System (Microsoft Dynamics (MD) system).

The Dynamics platform currently ingests testing data - record of a positive test - from the central test registry in the Business Services Organisation. This testing data will have come through Northern Ireland regional laboratory information systems (currently described as Pillar 1 testing), or the National Testing programme (currently described as Pillar 2 testing). The constructed Analytics Platform may include other sources of testing in the future, including Antibody serology and screening testing. Decisions regarding the expansion of testing regimes are beyond the remit of this document. This may include further additional National (UK) pillars if testing is expanded to include Northern Ireland.

As set out above contact tracing is an established public health tool to respond to infectious diseases nationally and internationally. While the PHA has much experience in contact tracing in relation to communicable diseases and outbreaks, the contact tracing service for COVID 19 is of a much larger scale and longer duration. However, PHA health protection expertise and knowledge is central to the development and management of this programme. Alongside this PHA is working with Digital Health NI (DoH and Health and Social Care Board (HSCB) E-Health) and Business Services Organisation IT Service (BSO ITS), to bring in expert technical knowledge and advice in respect of the IT system development, implementation and management.

4.2 Data Controllers and Processors

All of the data processors are appointed under Data Processors Agreements in compliance with Article 28 of the GDPR. The PHA is the data controller, as it is responsible for running the Contact Tracing Service and Analytics Platform, identifying the personal data to be collected, which individuals it is collected about, and how it is used. Please see Appendix A for full details.

Contracts and Memorandum of Understanding (MOUs) are in place to govern relationships with the above data processors and sub-processors, which set out the obligations of each party and the data controller's obligations and rights with regard to the data that is being processed. All contracts adhere to established BSO Procurement and Logistics Services (PaLs) processes and legal input provided by BSO Department of Legal Services (DLS).

All data processing takes place within the EEA area, and as such is subject to legislation in the form of the General Data Protection Regulation (GDPR).

4.3 Purpose of processing

The primary purpose of the processing of this data is to reduce the risk of the spread of COVID 19 in Northern Ireland by:

- Promptly identifying confirmed cases and their close contacts; and advising cases and close contacts to self-isolate and how to access testing if appropriate.

- Identifying clusters or outbreaks of infection (that is individuals with confirmed COVID-19 who are linked in time, place or person). If a suspected cluster of COVID-19 is identified by the Contact Tracing Service, the specialist Health Protection Team within the PHA are notified. If this cluster is determined to require additional measures or input, Health Protection colleagues will establish an Incident Management Team (IMT) to consider what additional steps are required to minimize further spread of COVID-19 in that setting.

- Surveillance (through bringing together a range of data about the disease in a timely manner, to inform decisions and actions across the public health system to help control the spread of the disease. This will include understanding the areas of the country which are most affected by an outbreak, whether particular groups of people are affected, whether symptoms are getting more severe, when the outbreak might have peaked and helping to predict how the outbreak will progress based on a range of different scenarios.

- The information within the Analytics Platform permits the automated production of investigations that will help to quickly identify those affected and the areas at risk from COVID 19. This facilitates rapid localised 'R' estimates and therefore less onerous mitigations can be introduced where needed.

It is important to be able to understand the pattern of cases and contacts, in terms of characteristics such as age, gender, occupational setting and geographical area. This is undertaken using a range of modelling and statistical techniques, including mapping of data to spot patterns. The analysis of the data is important to inform PHA actions (including the identification and management of clusters) and to inform the DoH (through high-level reports and trends) and therefore government policy responses.

The analytics system receives a continuous stream of data from the contact tracing information system to aid cluster management and surveillance. It was impractical to use anonymized or pseudonymised data as some analysis requires data linkage on factors such as name. Access to basic patient demographics (e.g. name, age, address, occupation etc.) is essential to allow a rapid risk assessment to be carried out. Information is assessed in terms of time, place and person (e.g. name, age, address, occupation etc.) without this information you cannot effectively associate cases with likely transmission.
COVID outbreaks and facilitates the emergency public health response that is necessary to deal with this pandemic. Given the huge number of calls expected and happened a system was required that automated the graphing (visual localisation) of COVID clusters. This is dependent upon having full details of each citizen affected, right down to their residency and full demographics. Only with this information is it possible for health protection to accurately and rapidly detect COVID clusters and to respond rapidly preventing extension of the outbreak. The tool facilitates this in a graphic way which is easy for human being to understand and is used additively to the standard data collection to facilitate rapid response. The use of full patient demographics aids identification of related individuals and facilitates rapid back tracing of those that have been contacts and then cases. Going forward the analytic platform is the primary public health clinical tool for the management of the COVID pandemic. It would be inconceivable that we could cope with this level of disease without an automated mechanism of displaying where cases and contacts have occurred. The analytics platform has facilitated that and has become and integrated part of the response to the COVID pandemic. The use of patient demographics in this way will shorten the length of time we suffer from COVID and will save lives. This process would not be as efficient or effective if no personal data was used. Therefore in the balance of risk it would be negligence of us not to use it as efficiently as possible to protect the public. As we have outlined there are multiple mitigations in place to make this as secure as possible.

HPZone is an established, business as usual product used by PHA Health Protection for the management of all small outbreaks of infectious disease. It was serviceable as a BAU product up until this pandemic when it became clear that the sheer volume of cases made its use as a primary platform impossible. It has continued to have a role in COVID pandemic management for the creation of Cluster Identifiers. Although consideration is being given to the automatic upload of relevant data to HPZone it is unlikely that this would become servable in the timeframe of this pandemic. That is why we have utilised the analytic platform as listed above as this limits the risk of data migration issue.

Anonymised data may be shared with other organisations (eg DoH, universities etc) for the purposes of planning and research related to COVID 19, in line with established processes.

4.4 Contact Tracing Service

The core contact tracing staff are PHA employees recruited specifically for their skills that match the requirements of the role. However, during the pilot phase, a number of re-deployed HSC staff were trained in contact tracing and staffed the centre on a rota basis. If the number of confirmed cases increase substantially, part of our contingency plan will be to increase the core staff with these trained HSC staff who worked in the pilot. Additionally, we have trained a number of HSC Trust bank nurse staff in contact tracing to increase our capacity if required.

The following staff roles exist within the PHA Contact Tracing Centre:

Clinical Lead

1. Advises on clinical complex issues
2. Leads on cluster management

Contact Tracing Centre Manager-

1. Allocates cases to callers
2. Advises callers on non-clinical complex calls
3. Reviews database for clusters
4. Refers clusters and complex calls to Health Protection Consultant

Contact tracers

1. Call cases/contacts
2. Gather information on contacts.
3. Enter data on database

Admin Support

1. Provides admin support to the team

- Managerial supervision of contact tracers is provided by The Contact Tracing Manager.

- There is ongoing ‘open door’ policy for clinical supervision with the clinical medical staff on site.

- The clinical lead is a medical clinician (public health doctor or GP).

- The contact tracers are comprised from the following professions: nurses, Environmental Health Officers, social workers, Allied Health Professionals along with some doctors and dentists.

- Staff are governed by their relevant professional codes of conduct as well as the terms of their employment with the PHA. The contract of employment includes a clause on confidentiality, as follows:

> "*In the course of your employment you may become aware of medical and other information relating to patients, clients, residents, visitors and other members of staff. Such information must not be divulged to anyone other than those employees of the PHA or others clearly associated with the provision of the PHA's services authorised to receive it in the course of their duties.*
>
> *Any breach of confidentiality is viewed as a serious matter and will lead to disciplinary action in accordance with the PHA's agreed procedure. If in doubt at any time, you should ask your manager for guidance*."

- All HSC staff are also required to comply with the HSC Code of Conduct. (Appendix E)

- All contact training staff are required to complete a one day intensive training course before commencing 'live' contact tracing. This includes a dedicated session on data protection and information governance (developed with input from PHA Information Governance Manger), as well as supervised practice with the Education Lead. Training is delivered by a dedicated trainer (Education Lead) from the HSC Leadership Centre (see appendix J).

- All staff (including bank) must complete the regional HSC online information governance awareness and IT security training modules. (Or, if coming from another HSC organisation, have completed the training within the previous year). In addition, they are also required to complete health and safety, fire safety and risk management training in the same way as other PHA staff. All those involved in the use of the Analytic platform have also undergone information governance training and are PHA employees (including those with honorary contracts).

Common Law Duty of Confidentiality

The staff working in the Contact Tracing Service and with the Analytics Platform are governed by their professional codes of conduct and HSC contractual terms, including the duty of confidentiality.

Under common law, if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent. In practice, this means that all patient/client information, whether held on paper or computer, must not normally be disclosed without the consent of the patient/client. However, there are several very specific circumstances that makes the disclosure of confidential information lawful, including the sharing of necessary information with other health and care professionals and agencies where the interests of patient safety and public protection override the need for confidentiality.

The CTS may need to share personal information in the interests of individual patient safety or to protect the wider public. However, it is only in exceptional cases where the details of the person who has tested positive (the 'confirmed case') and has provided their information, would need to be shared with another health professional or agency. In so far as it is applicable, personal data will only be shared where it is absolutely necessary for health protection for the individual, or for wider public protection in controlling and reducing the spread of COVID-19 and safeguarding the health and wellbeing of other individuals who the 'confirmed case' may have been in contact with.

4.5 Contact Tracing Processing

The functionality delivered by the Contact Tracing Information System and Digital Self Trace is designed to support the manual contact tracing operation in Northern Ireland works as follows:

1. The contact tracing process is triggered by receipt of positive COVID 19 test (virology) results into the CTIS.

2. NI residents who have received a positive COVID 19 test result and are over the age of 16 will be sent an SMS message, from HSCtracing, inviting them to use Digital Self Trace.

The SMS message will be sent using the Gov.UK notify service. The message will contain a code that the citizen needs to enter, that will then be used for linkage purposes once the data is received into the CTIS. The purpose of the Digital Self Trace system is to enable information about the close contacts (criteria listed below) to be collected more quickly, and to make better use of contact tracers time. This will enable the CTS to be able to manage increased volume of work, and help ensure that people are contacted as quickly as possible to inform them of the need to self-isolate to reduce the spread of the virus. The data submitted through DST may be reviewed during a contact tracer's phone call with the positive case.

3. The PHA Contact Tracers will contact NI residents who have received a positive COVID 19 test result (calls are outbound only – there is no function for citizens to contact the centre). The purpose of the phone call is to identify anyone who the

confirmed case has been in contact with during the time that they were likely to be infectious (or validate data entered onto DST). Contacts may include someone:

- Who lives with the confirmed case;
- Who has been in direct contact with the confirmed case or their bodily fluids (eg droplets from a cough or sneeze); or
- Who has been within 2 metres of the confirmed case for more than 15 minutes.

If the citizen has completed Digital Self Trace the contact tracer will be able to see the data and will be able to validate it during the call. They will also be given relevant public health advice and information during the call.

4. Following assessment of the information provided by the confirmed case (including details provided about their contacts) the PHA CTS will close the data collection for the positive case and trigger an automated process sending all contacts, for that case, a SMS message. The SMS is addressed (using name supplied by positive case) and states that they are a close contact and need to self-isolate.

5. The PHA CTS may also call their contacts and provide advice on what they should do (including advice on self-isolation and testing).

All calls from the PHA CTS will come from the number 028 9536 8888 and all SMS messages come from HSCtracing.

The Northern Ireland Expert Modelling Group (led by the DoH Chief Scientific Adviser) has advised that around 2000 people each day may have one of the three key symptoms of the disease, and that under normal circumstances (that is without restrictions imposed by lockdown), each confirmed case may have up to 30 contacts. However, the number of positive test results (and therefore the number of confirmed cases) and the number of contacts, is likely to fluctuate over the coming months, depending on the extent of restrictions in force at the time and compliance with social distancing and other measures.

The PHA CTS will be required until a vaccine is developed and a mass vaccination programme implemented or there is sufficient herd immunity in order that the disease may be controlled. This is likely to be at least two years.

4.5.1 Data Sources

The following four sections outline the different data sources:

4.5.1.1 Positive COVID 19 Test

Positive COVID 19 tests are provided to the CTS by the Central Test Registry (CTR). The Central Test Registry (See appendix B for schema) is part of the existing HSC data warehouse, and includes COVID19 results received from:

- the HSC Laboratory Information Management Systems and
- the National Testing Initiative. (Results from the National Testing Initiative are centrally collected and then distributed to regions via the National Pathology Exchange (NPEx); only those test results relating to NI residents are sent to the NI Central Test Registry. Results are passed from the National Pathology Exchange (NPEx), to the HSC Test registry hosted and administered by the Business Services Organisation (BSO) who are data processors for this data, on behalf of PHA, the data controller for COVID 19 test data. The portal, and testing data sit outside the CTS architecture and this processing is covered off under separate Information Governance arrangements. The flow of this data from the National Testing Initiative is governed by a S255 letter between DoH, PHA and Department of Health and Social Care (England)

The results from the two sources contain different data sets with neither set providing all the information required for contact tracing. One of the purposes of the central test registry is to provide a complete dataset. The registry receives all COVID 19 test results (both positive and negative) from the various laboratory sources, combines the results into a single register which can match test results to patient demographics (validating Health and Care Numbers and allocating test results to patient records where no Health and Care Number has been recorded in the original data set) and enhances the datasets by acquiring matched telephone numbers and any Next of Kin details, from existing HSC information systems (See Appendix I for further details).

The central test registry provides a data extract of positive COVID 19 test results (only) to the Contact Tracing Information System. This extract is transferred within the secure HSCNI network (using File Transfer Protocol, FTP) to a specified PHA folder (secure network drive) that has restricted access. The extract is sent 7 days a week at 6 allotted times: 06:00, 08:30, 10:35, 12:40 15:00 and 22:00. (For example, the 06:00 file will contain all positive results received by the registry since 22:00 the previous day). The timing intervals are based on observation of result timings and frequency eg in general more test results are received in AM rather than PM; timing intervals can be easily scaled up and down as required by the Contact Tracing Service.

The extract provides the following fields, which may or may not be populated depending on a number of key factors (see detailed description in section 5.2)

- CTR ID
- Surname
- Forename
- DOB
- Gender
- HCN
- Date of Death

- Address 1
- Address 2
- Postcode
- City
- National Results Contact Number
- Additional Contact Numbers
- Contact Email
- Next of Kin
- Test ID
- Date of Sample
- Lab Result
- Labs source
- Date Booked in
- Date of Report
- Patient Cat Type
- Care Home Code
- Care Home Name
- Date Loaded
- Key Worker

All Northern Ireland test results received by the PHA Contact Tracing Information System come from the Central test registry which is part of the HSC\BSO Data Warehouse. The Contact Tracing Information System is configured to upload the contents into specific fields within the CTIS. Each record in the extract will be loaded into the system as a new contact; upload performs data validation which rejects records that fail. Any rejected records are manually reviewed by PHA CTS and actioned appropriately (for example if DOB came through in American rather than English format, or if a mobile number came through without the initial '0', this could be manually corrected to ensure an accurate record is loaded into the system).

The extract form the Central Testing Registry only contains the data items required by the contact tracing team, to enable them to make contact with the individual (and confirm it is the correct person), and to help identify links with other cases (as part of cluster management) and does not include the complete set of data held by the central test registry.

Appendix I outlines BSO assurances on quality and processes.

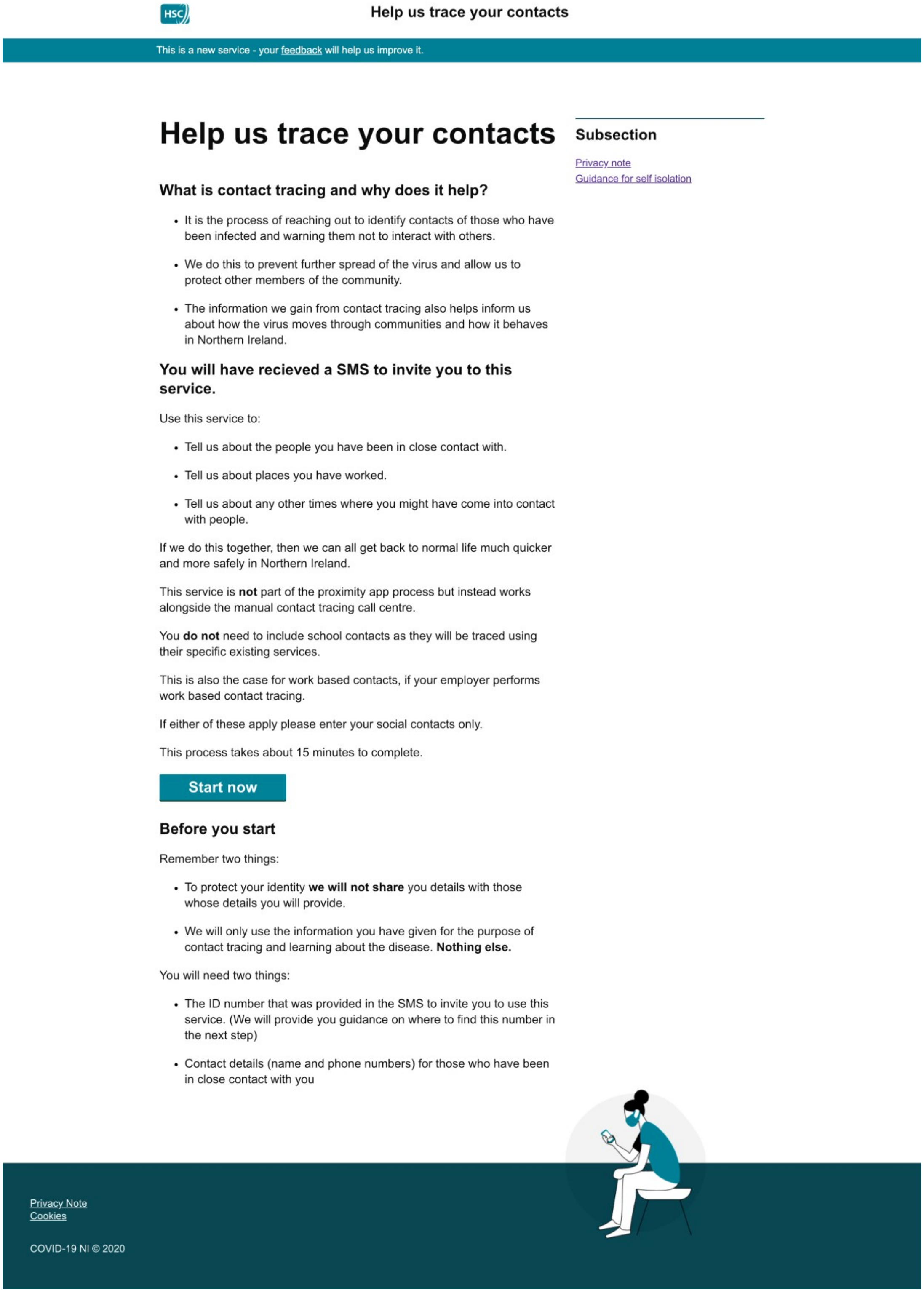
4.5.2 Data collected from Confirmed Cases

Once a new confirmed case (person who has tested positive for COVID 19) has been loaded onto the system it will be assigned by a CTS administrator to a contact tracer's work queue.

4.5.2.1 Data collected via Digital Self Trace

The successful loading will also trigger an SMS message, from HSCtracing, inviting the citizen (age 16 and above) to complete Digital Self Trace (DST).

See below front screen:



Help us trace your contacts

This is a new service - your feedback will help us improve it.

Help us trace your contacts

What is contact tracing and why does it help?

- It is the process of reaching out to identify contacts of those who have been infected and warning them not to interact with others.
- We do this to prevent further spread of the virus and allow us to protect other members of the community.
- The information we gain from contact tracing also helps inform us about how the virus moves through communities and how it behaves in Northern Ireland.

You will have recieved a SMS to invite you to this service.

Use this service to:

- Tell us about the people you have been in close contact with.
- Tell us about places you have worked.
- Tell us about any other times where you might have come into contact with people.

If we do this together, then we can all get back to normal life much quicker and more safely in Northern Ireland.

This service is **not** part of the proximity app process but instead works alongside the manual contact tracing call centre.

You **do not** need to include school contacts as they will be traced using their specific existing services.

This is also the case for work based contacts, if your employer performs work based contact tracing.

If either of these apply please enter your social contacts only.

This process takes about 15 minutes to complete.

Before you start

Remember two things:

- To protect your identity **we will not share** you details with those whose details you will provide.
- We will only use the information you have given for the purpose of contact tracing and learning about the disease. **Nothing else.**

You will need two things:

- The ID number that was provided in the SMS to invite you to use this service. (We will provide you guidance on where to find this number in the next step)
- Contact details (name and phone numbers) for those who have been in close contact with you

Subsection

Privacy note

Guidance for self isolation

Privacy Note

Cookies

COVID-19 NI © 2020

The citizen will be guided to provide the following information on their contacts (they will not be asked for anything additional to what would be asked during a call with a Contact Tracer).

If the citizen chooses to use Digital Self Trace then they will be asked to input the following information about themselves:

- name,
- age
- postcode,
- contact telephone number
- ethnic group
- Employment; type of employment, employer name, employer telephone number, and in particular if they are a health or social care worker. They are also asked have they been in work in the last 7 days;
- accommodation type; if they are currently in hospital, or living in a Care Home or any other shared accommodation;
- Symptomatic (Y/N)
- Isolation behaviours
- whether or not they travelled outside Northern Ireland in the 14 days before their symptoms appeared (or test, if no symptoms).

If the citizen chooses to use Digital Self Trace then they will be asked to input the following information about their contacts:

- Name
- Mobile or other phone number
- Postcode
- Household member?
- Do they work in healthcare?
- Has the 'contact' been unwell since the confirmed case last saw them (to the best of their knowledge)
- Under 16?
- Time frame of contact (within 24hours up to five days ago or longer)
- Type of contact
- Contact Location (settings, such as a sports venue or a restaurant)

4.5.2.2 Data collected via phone call from the Contact Tracing Service

The contact tracer will then make contact with each 'confirmed case' via a phone call. All calls from the PHA CTS will come from the number 028 9536 8888 and all SMS messages come from HSCtracing.

Data will then be collected or verified from the confirmed case by the contact tracers during telephone call(s).

When the contact tracers telephone the confirmed case, they will firstly seek to verify information already received (name, address, postcode, and date of contact). The contact tracer will ask the confirmed case for some additional information as follows:

- their occupation and place of work, and in particular if they are a health or social care worker;
- if they are currently in hospital, or living in a Care Home or any other shared accommodation;
- the date and time of first symptoms, date they started to self-isolate and
- whether or not they travelled outside Northern Ireland in the 14 days before their symptoms appeared (or test, if no symptoms).

They will be provided with advice, including about self-isolation.

If the citizen hasn't completed DST then the tracer will ask the confirmed case to provide the following information about their contacts:

- Name
- Mobile or other phone number
- Work address if known
- Shared residential address if known
- Date of contact
- Type of contact
- Do they work in healthcare
- Has the 'contact' been unwell since the confirmed case last saw them (to the best of their knowledge)

They will also be asked about any places where they have been in contact with others, but would not be able to provide names. If they identify a setting, such as a sports venue or a restaurant, they will be asked if they can provide a contact name.

For example, if a Gaelic player tests positive and tells the contact tracers that he has been training/playing, but does not know all the close contact details, he will be asked to provide a club contact. If he doesn't know this, the CTS will seek to contact the governing organisation and ask for a contact. When contact is made the CTS will ask the organisation for details of who was present at that time and place (the name of the contact is not given). Once the list of names and contact details, for that time and date, are received, the contact tracers will check to ensure that the contact is listed, and will assess who is a close contact and only contact those individuals.

In the same way, if the confirmed case has visited a hospitality venue (for example a restaurant), the venue will be contacted to ask for their list of staff and customers/visitors and their contact phone numbers (where there has been a group of people, only the contact number of the lead member of the group will be provided). The Department of the Economy has issued guidance for the hospitality industry in NI that can be found at: https://www.health-ni.gov.uk/hospitality

Where a confirmed case identifies potential contacts in a school, the CTS will contact the school to identify who is at risk and should therefore be contacted. In respect of children, the school will be asked to provide the contact details for the child's parent or legal guardian.

4.5.3 Data collected from 'Contacts'

Once all the data collection has been successfully completed the PHA CTS will close the data collection for the positive case and trigger an automated process sending all contacts, for that case, a SMS message. The SMS is addressed (using name supplied by positive case) and states that they are a close contact and need to self-isolate.
The tracer may make contact with a close contact via a phone call. Data would then be collected from the close contacts by the contact tracers during telephone call(s).

During the call the Contact Tracer will confirm the details supplied (eg name, contact details), and seek some additional information about the close contact, including if the person is currently in hospital or living in a Care Home, or any other shared accommodation and their occupation and place of work. They will be asked if they have symptoms, if they are isolating and whether or not they travelled outside Northern Ireland.

This minimum data set obtained from the central test registry along with the data received from people who have tested positive and their contacts during phone calls with the Contact Tracers is listed in section 5.2. The data collected and stored is the minimum amount required for the purposes of individual contact tracing, cluster management and surveillance. Further details on data flows are provided in the appendix F.

4.5.2 Other Data Sources

4.5.4.1 Data supplied through Port Health systems, in respect of passengers on ship or airplanes

Port Health (management of contacts of individuals with a communicable disease who have travelled by ship or airplane) is an established and routine process operated by the PHA Health Protection Team. In the case of COVID 19, the Contact Tracing service will submit a request to the airline or maritime operator requesting a copy of the passenger manifest from the airline or maritime operator for a specific flight/commercial maritime vessel, as identified by the positive case through contact tracing.

The passenger manifest is password protected by the airline or maritime operator. Once received, the Health Protection Consultant reviews the list, advises on clinical complex issues and leads on cluster management. The contact tracers will telephone the relevant contacts as above.

4.5.4.2 Data from other jurisdictions

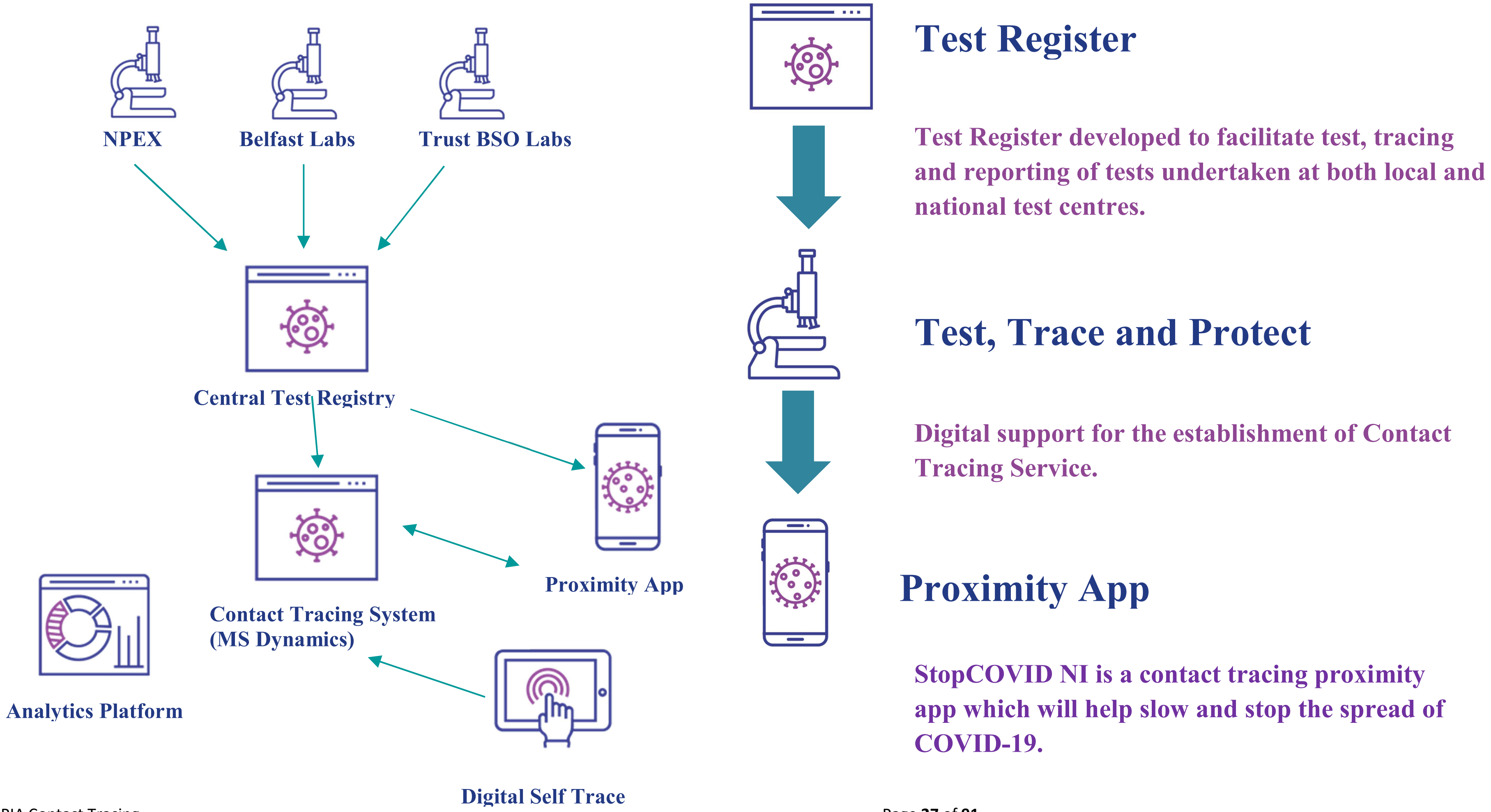
Data may also be received from Health Protection bodies in England, Scotland, Wales or Republic of Ireland in respect of NI residents who have been in contact with someone who has tested positive in one of these jurisdictions. (Also reference section on transfer of data out)

4.5.4.3 Trust employees

Explorative work is underway to collect data on contact tracing currently performed within HSC Trusts in respect of exposure to COVID 19 on Trust premises eg employees.

5 Data Flows and Technical Architecture

Contact tracing system is one of a number of digital TTP Components that are interlinked. See below diagram A:



Test Register

Test Register developed to facilitate test, tracing and reporting of tests undertaken at both local and national test centres.

Test, Trace and Protect

Digital support for the establishment of Contact Tracing Service.

Proximity App

StopCOVID NI is a contact tracing proximity app which will help slow and stop the spread of COVID-19.

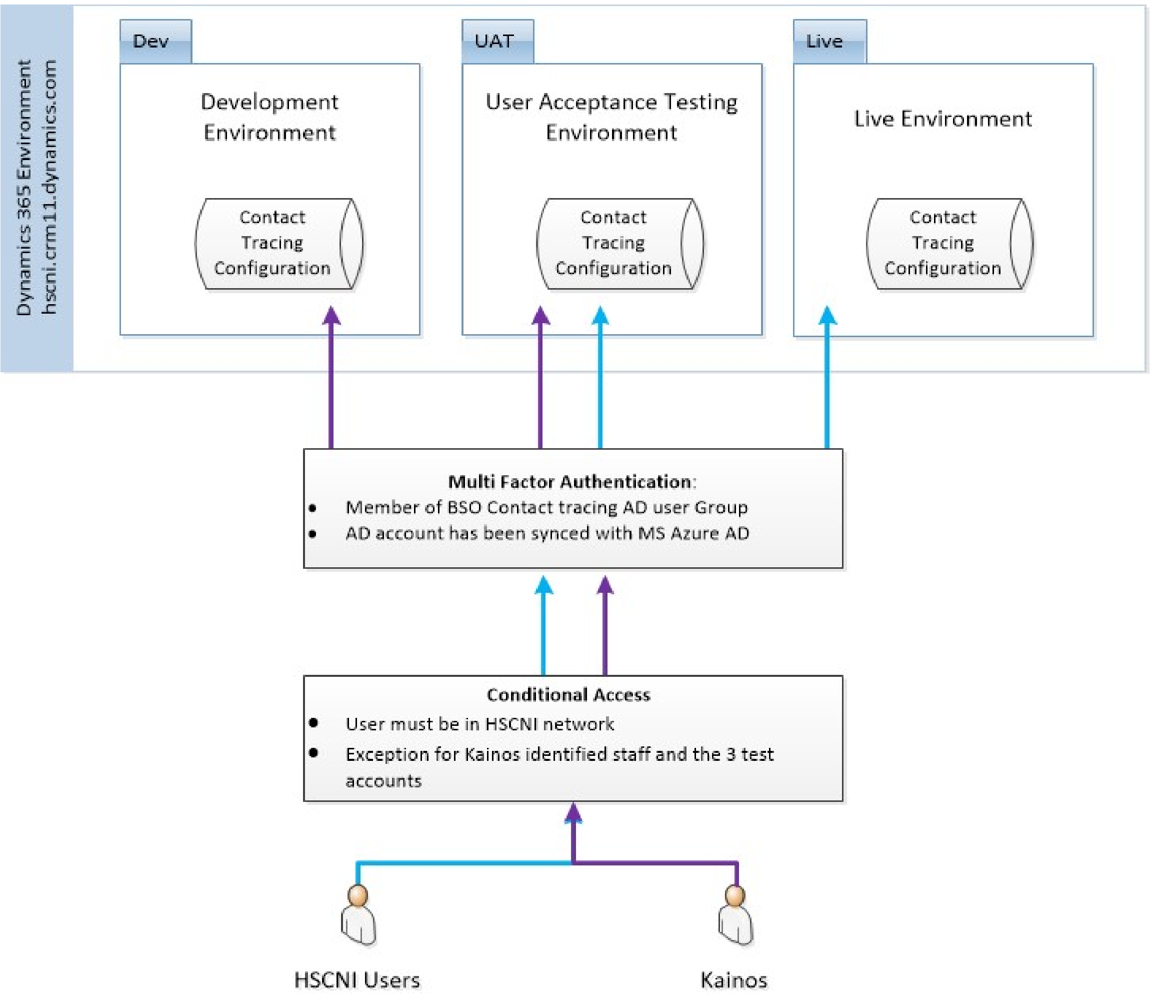
5.1 Technical Architecture

5.1.1 CTIS Contact Tracing Information System (CTIS)

The PHA Contact Tracing Information System, holds all the data received from the sources outlined in section 4. It is hosted in the isolated cloud storage solution provided by Microsoft. This environment contains three different instances:

1. Development
2. Testing
3. Live (also known as production)

See below diagram B:


Dynamics 365 Environment
hscni.crm11.dynamics.com
Dev
Development Environment
Contact Tracing Configuration
UAT
User Acceptance Testing Environment
Contact Tracing Configuration
Live
Live Environment
Contact Tracing Configuration
HSCNI Users
Kainos

Multi Factor Authentication:

- Member of BSO Contact tracing AD user Group
- AD account has been synced with MS Azure AD

Conditional Access

- User must be in HSCNI network
- Exception for Kainos identified staff and the 3 test accounts

Access to these areas are restricted and only staff working in the CTS (identified and approved by the PHA) with accounts authorised by BSO ITS can gain successful access.

Only computers located within the HSCNI network can be used to access the systems (exception of the approved 3rd party providers who access, the instances where they have authorised access, via secure VPN connections). Only specific named PHA staff who work in the Contact Tracing Service and have an HSCNI Active Directory access account, have access to the Contact Tracing Information System.

Three instances:

1. Development instance will only be accessible by the authorised and named Kainos (3rd party developer) accounts and used for development reasons.

2. Testing instance will be accessible to Kainos accounts and authorised and named HSCNI accounts belonging to staff assigned to COVID-19 tracing centre. The main use for this system is testing enhancement and training purposes.

3. The Live instance is only accessible by the authorised and named HSCNI accounts belonging to staff working in the CTS. This instance contains the live data and is the only instance that does.

There will be no real data used in the development and testing stage; these instances will contain fictitious dummy data.

5.1.2 Digital Self Trace (DST)

The digital self-trace system is a web app which offers COVID -19 positive citizens (over 16 years old) the ability to report their contacts digitally. It is an additional data source available to the contact tracing information system; the digital data requested is a slightly reduced data set than would be verbally requested.

It is hosted in Microsoft Azure isolated cloud storage solution provided by Belfast Health and Social Care Trust (BHSCT). The webapp is publically accessible by a URL:

https://trace.COVID-19.hscni.net/

There are no restrictions on the live URL and it is open to public. To proceed a validated test code is required, without this no data can be entered. All data is stored in the browser cache while being completed and no data is transmitted until the final page is reached and the submission button is clicked. Data transmitted to Microsoft Azure and then submitted to CTIS via the API (see section 5.2 for architecture diagram)

When data is received by CTIS it is first electronically verified via a matching criteria. This criteria is currently using the test number as contact tracers will be reviewing the details provided before any contact (SMS and potentially a phone call) will be made with close contacts. In future if this manual validation set is removed additional matching criteria will be added.

If these match to an existing record within CTIS the data is added to that file and an onscreen flag is added to show that this is digital self-trace data. If the criteria is not matched then the record will be added to the triage queue. This queue is also used for rejected records from the CTR extract (duplicates). This queue is monitored by CTC staff and records are manually reviewed. Outcome of the manual review is record is accepted, eg Smyth and Smith, or it is rejected and deleted from CTIS. Only identified users within the contact tracing service have the correct access rights to access the triage queue. See Appendix K for data flows of Digital Self Trace

There is a DST Test (pre-production) environment but it is restricted to an allowed list of IP's (this is controlled by PHA and enabled by Kainos):
https://HSC-TraceApp-frontdoor-prod.azurefd.net

The test URL is attached to the Test CTIS and no real data is used in the testing stage; these instances contain fictitious dummy data.

5.1.2.1 PECR Guidelines

DST has a cookie policy which is accessible from the front screen. The cookie policy, see Appendix L, includes information on

- say what cookies will be set;
- explain what the cookies will do; and
- obtain consent to store cookies on devices.

Within DST no data for analytics is being stored, google analytics is being used purely to track usage of the site. Cookie policy, accessible from within DST clearly states what is being stored and provides the citizens with an opt out option. The cookie policy is included in appendix L (Section 5.6.2 covers PECR for SMS messaging).

5.1.3 SMS Messages Gov.UK Notify

Gov.UK Notify is being used to send both positive case and close contact SMS messages. This is also the platform used by STOP COVID NI app.

GOV.UK Notify is built for the needs of government services. It has processes in place to:

- protect user data
- keep systems secure
- manage risks around information

Data is encrypted:

- when it passes through the service
- when it's stored on the service

Any user data you upload is only held for 7 days as per GOV.UK notify processes. For DST this would be the positive case name and phone number. This data is held by GOV.UK notify and is only accessible via the website.
Notify complies with data protection law. To make sure it stays compliant, there are regular legal reviews of the services.

CTIS integrates via the GOV.UK Notify API. For positive cases the data passed is:

1. Forename and surname
2. Test ID

Message template:

> Dear ((firstName)) ((lastName))
> You recently tested positive for COVID-19.
>
> Please self-isolate.
>
> We now need your help to trace your contacts.
> Please use the Digital Self-Trace service: trace.covid-19.hscni.net
> Use DST code: ((uniqueID)) (one time use)

Reminder SMS Message (if no response nor no contact made by manual contact tracing 5 hours after initial text message within texting hours 07:30 and 21:30):

> Dear ((firstName)) ((lastName))
> You recently tested positive for COVID-19.
>
> We sent you a message asking for your help to urgently trace your contacts. This is a reminder.
>
> Please use the Digital Self-Trace service: trace.covid-19.hscni.net
> Use DST code: ((uniqueID)) (one time use)

For close contacts the data passed is only the forename and surname. Message template:

> Dear ((firstName)) ((lastName))
>
> You have been in close contact with someone who has COVID-19.
>
> You are at high risk of having and spreading it. Self-isolate now for x days.
>
> For more guidance visit covid-19.hscni.net/closecontact/

Access to the GOV.UK notify website is controlled by PHA. Users are added and assigned required permissions. User access to the system is via two-factor authentication:

- email address and password
- a text message code that Notify sends to your phone

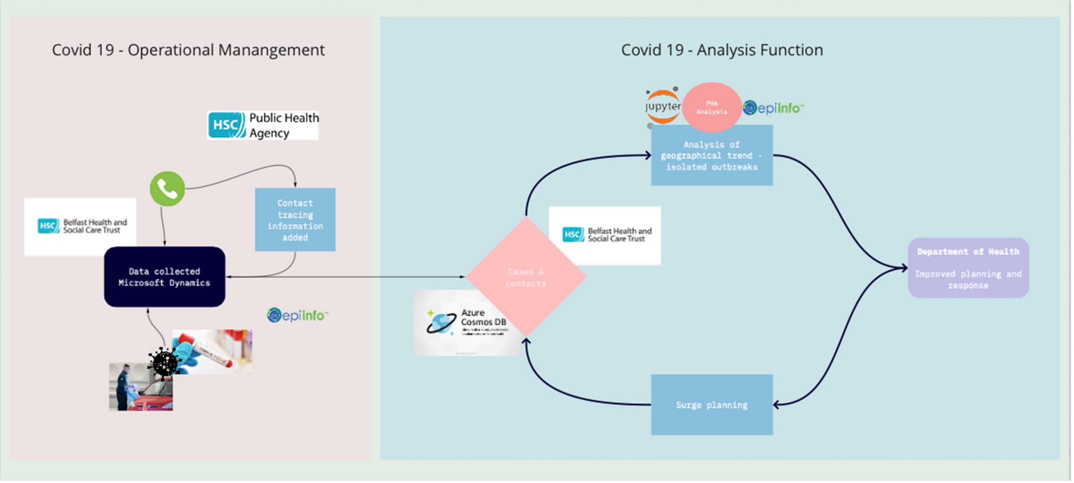
Selected authorised Contact Tracing staff, contact tracing manager and admin lead, have access to this website; they are bound by the existing controls and policies and professional regulatory Codes of Conduct.

Sender ID of these messages is HSCtracing and both the sender ID and message content has been reviewed by National Cyber Security Centre.

5.1.3 Analytics Platform

This pandemic has highlighted the need for real time data to enable the identification and the understanding of the patterns of transmission so that they may be successfully interrupted. This information is critical to the Public Health response and represents the quickest way to locally adjust guidance, reduce COVID 19 spread and save lives. The analytics platform has become the quickest and most effective way of identifying local area involvement and therefore allowing rapid targeted responses. This is a critical step to allow live analysis of COVID 19 case numbers as they are reported and enables more accurate contact tracing and cluster analysis.

The analytic platform has been built in a Microsoft Cloud hosted environment within Belfast Health and Social Care Trust tenancy, hosted in a UK data Centre. This environment has been securely Penetration tested and is GDPR compliant. The image below gives a high level overview of how the information used in the Analytics Platform is compiled.


Covid 19 - Operational Manangement
HSC Public Health Agency
HSC Belfast Health and Social Care Trust
Contact tracing information added
Data collected Microsoft Dynamics
epiinfo
Covid 19 - Analysis Function
jupyter
PHA Analysis
epiinfo
Analysis of geographical trend - isolated outbreaks
HSC Belfast Health and Social Care Trust
Cases & contacts
Azure Cosmos DB
Department of Health
Improved planning and response
Surge planning

The platform is based on Microsoft Azure, which is a cloud platform that can build, run, and manage applications. Microsoft Azure Cosmso DB is used as the overall database for the Analytics Platform.

Restricted access virtual computers are utilised to allow secure analysis of data. This will be facilitated by jupyter (open source statistical software) notebooks using a containerised version of R statistical software. Jupyter is analytics software used by analysts to investigate outbreaks and guide intervention.

5.2 Data Collection

The data collected and held by the contact tracing service will relate to individuals who have tested positive for COVID 19 in NI and those they are able to identify as having been in close contact with, during the period of infection. If an individual has been in contact with someone outside of Northern Ireland the information on their contacts will be passed onto the relevant authorities under current data sharing agreements. In the exceptional cases where the name of the confirmed case needs to be shared, they will be informed about this.

There are five key types of data within the CTIS:

1. Central Test Registry
2. Procedural fields
3. Data verified/collected from confirmed case
4. DST Data
5. Data verified/collected from close contacts

Central Test Registry data supplied is as follows:

Field Title	**Additional Information**
CTR ID	Central Test Registry generated unique ID, retained for data integrity not visible from front end
Surname	Central Test Registry verified data from HSCNI sources (see diagram A) for both NPEX and trust lab results. For NPEX test if a positive case is previously unknown to HSCNI then this will contain the value provided during test booking.
Forename	Central Test Registry verified data from HSCNI sources (see diagram A) for both NPEX and trust lab results. For NPEX test if a positive case is previously unknown to HSCNI then this will contain the value provided during test booking.
DOB	Central Test Registry verified data from HSCNI sources (see diagram A) for both NPEX and trust lab results. For NPEX test if a positive case is previously unknown to HSCNI then this will contain the value provided during test booking.
Gender	Central Test Registry verified data from HSCNI sources (see diagram A) for both NPEX and trust lab results. For NPEX test if a positive case is previously unknown to HSCNI then this will contain the value provided during test booking.
HCN	Central Test Registry collected data from HSCNI sources (see diagram A) for both NPEX and trust lab results. This field may not be populated if positive case is previously unknown to HSCNI.
Date of Death	Central Test Registry collected data from HSCNI sources (see diagram A) for both NPEX and trust lab results. This field will only be populated if positive case is previously known to HSCNI and a date of death is recorded on a HSCNI system.
Address 1	Central Test Registry verified data from HSCNI sources (see diagram A) for both NPEX and trust lab results. For NPEX test if a positive case is previously unknown to HSCNI then this will contain the value provided during test booking.
Address 2	Central Test Registry verified data from HSCNI sources (see diagram A) for both NPEX and trust lab results. For NPEX test if a positive case is previously unknown to HSCNI then this will contain the value provided during test booking.
Postcode	Central Test Registry verified data from HSCNI sources (see diagram A) for both NPEX and trust lab results. For NPEX test if a positive case is previously unknown to HSCNI then this will contain the value provided during test booking.
City	Central Test Registry verified data from HSCNI sources (see diagram A) for both NPEX and trust lab results. For NPEX test if a positive case is previously unknown to HSCNI then this will contain the value provided during test booking.
National Results Contact Number	NPEX collected data and placed into primary contact number; this field will be empty for trust lab results
Additional Contact	Central Test Registry collected data from HSCNI sources (see diagram A) for trust lab

Numbers	results; this field will be empty for NPEX results
Contact Email	NPEX collected data, this field will be empty for trust lab results
Next of Kin	Central Test Registry collected data from HSCNI sources (see diagram A) for both NPEX and trust lab results. This field will only be populated if positive case is previously known to HSCNI and a date of death is recorded on a HSCNI system.
Test ID	NPEX generated unique ID, this field will be empty for trust lab results; retained for data integrity not visible from front end
Date of Sample	Central Test Registry provided data;
Lab Result	Central Test Registry provided data; all tests will be positive as that is the criteria for the extract
Labs source	Central Test Registry provided data; identifies lab eg specific trust lab or NPEX
Date of Report	Central Test Registry provided data
Patient Cat Type	Central Test Registry provided data; identifies in patients
Care Home Code	Central Test Registry verified data from HSCNI sources (see diagram A) for both NPEX and trust lab results. For NPEX test if a positive case is previously unknown to HSCNI then this will contain the value provided during test booking.
Care Home Name	Central Test Registry verified data from HSCNI sources (see diagram A) for both NPEX and trust lab results. For NPEX test if a positive case is previously unknown to HSCNI then this will contain the value provided during test booking.
Date Loaded	Central Test Registry provided data; reflects date of extract
Key Worker	NPEX collected data, this field will be empty for trust lab results

Data collected by the Procedural fields:

Field Title	Primary Data Source	Additional Information
Status	Manually entered by contact tracers	Open, In progress, closed
Outcome	Manually entered by contact tracers	Successful/unsuccessful
Outcome – unsuccessful reason	Manually entered by contact tracers	Eg Tried 5 times within 48 hrs, Case episode duplicated etc
Date of call	Manually entered by contact tracers	
Call attempt number	Manually selected by contact tracers	
Timeline Title	Manually entered by contact tracers	Used by contact tracers to record call attempts details eg contact asked to be contacted tomorrow morning
Timeline Note	Manually entered by contact tracers	
Timeline Username	Manually entered by contact tracers	

Data verified/collected from confirmed case (Call 1)

Group	Field Title	Primary Data Source	Additional Information
Case – Demographics fields	First Name	Central Test Registry	Verified by contact tracer and updated if required
Case – Demographics fields	Last Name	Central Test Registry	Verified by contact tracer and updated if required
Case – Demographics fields	Email	Central Test Registry or Manually entered by contact tracers	Verified by contact tracer and updated if required
Case – Demographics fields	Primary Contact Number	Central Test Registry	Verified by contact tracer and updated if required
Case – Demographics fields	Alternative Contact Number	Central Test Registry	Verified by contact tracer and updated if required; if a local labs results tracer will move the telephone number from this field int the primary contact number
Case – Demographics fields	Address line 1	Central Test Registry	Verified by contact tracer and updated if required
Case – Demographics fields	Address line 2	Central Test Registry	Verified by contact tracer and updated if required
Case – Demographics fields	Address line 3	Central Test Registry	Verified by contact tracer and updated if required
Case – Demographics fields	City	Central Test Registry	Verified by contact tracer and updated if required
Case – Demographics fields	Postcode	Central Test Registry	Verified by contact tracer and updated if required
Case – Demographics fields	DOB	Central Test Registry	Verified by contact tracer and updated if required
Case – Demographics fields	Age		Calculated field using DOB
Case – Demographics fields	Gender	Central Test Registry	Verified by contact tracer and updated if required

Case – Demographics fields	Date of Death	Central Test Registry	Updated if required
Case – Demographics fields	GP Name	Manually entered by contact tracers	Only entered when GP interaction is required eg urgent health concerns identified during the call. GP contact is made by the clinical lead
Case – Symptom fields	Date of Onset	Manually entered by contact tracers	In the case of symptomatic patients, date of onset of symptoms
Case – Symptom fields	Date of Sample	Central Test Registry	Verified by contact tracer and updated if required
Case – Symptom fields	Date of Report	Central Test Registry	Verified by contact tracer and updated if required
Case – Demographics fields	HCN	Central Test Registry	Verified by contact tracer and updated if required
Case – Symptom fields	Result	Central Test Registry	All tests will be positive
Case – Symptom fields	HPZone Situation No	Manually selected by contact tracers	If the positive case is part of a cluster the allocated HPZone ID wi be added
Case – Demographics fields	Case Deceased	Manually selected by contact tracers	Yes or No
Case – Demographics fields	Designated Contact?	Manually selected by contact tracers	Yes or No; if yes proxy details are requested
Case – Demographics fields	Confirm U16?	Manually selected by contact tracers	Yes or No; if no proxy details are requested
Case – Demographics fields	Well enough to speak?	Manually selected by contact tracers	Yes or No; if no proxy details are requested
Case Proxy Details (only populated if required)	Proxy First name	Manually entered by contact tracers	If key answers are selected to Designated Contact?, Confirm U16? Or Well enough to speak?
Case Proxy Details (only	Proxy Last name	Manually entered by contact tracers	

populated if required)			
Case Proxy Details (only populated if required)	Proxy contact number	Manually entered by contact tracers	
Case Proxy Details (only populated if required)	Proxy Relationship	Manually entered by contact tracers	
Case – Symptom fields	Recently Tested for COVID19	Manually selected by contact tracers	Yes or No
Case – Symptom fields	Contacted about COVID19 result ?	Manually selected by contact tracers	Yes or No
Case – Symptom fields	Result provided by caller ?	Manually selected by contact tracers	Yes or No
Case – Symptom fields	Already completed tracing with someone else from PHA?	Manually selected by contact tracers	Yes or No
Case – Demographics fields	Ethnic Group	Manually selected by contact tracers	
Case – Employment fields	Occupation	Manually entered by contact tracers	
Case – Employment fields	Employer Name	Manually entered by contact tracers	
Case – Employment fields	Been @ work in last 7 days	Manually selected by contact tracers	Yes or No
Case – Employment fields	Healthcare worker?	Manually selected by contact tracers	Yes or No
Case – Employment fields	Direct Patient Contact?	Manually selected by contact tracers	Yes or No

Case – Symptom fields	Symptomatic (Y/N)	Manually selected by contact tracers	Yes or No
Case – Symptom fields	Self-Isolating?	Manually selected by contact tracers	Yes or No
Case – Symptom fields	Isolation start date	Manually entered by contact tracers	
Case – Symptom fields	Isolation end date	Manually entered by contact tracers	
Case – Location Information (one or many can be entered)	Location Description	Manually entered by contact tracers	Completed per location
Case – Location Information (one or many can be entered)	Location Address line 1	Manually entered by contact tracers	Completed per location
Case – Location Information (one or many can be entered)	Location Address line 2	Manually entered by contact tracers	Completed per location
Case – Location Information (one or many can be entered)	Location Address line 3	Manually entered by contact tracers	Completed per location
Case – Location Information (one or many can be entered)	Location City	Manually entered by contact tracers	Completed per location
Case – Location Information (one or many can be entered)	Location Postcode	Manually entered by contact tracers	Completed per location
Case – Location Information (one or many can be entered)	Location Category	Manually entered by contact tracers	Completed per location; options include Restaurant, Gym, Pub etc
Case – Location Information	Date Visited	Manually entered by contact tracers	Completed per location

(one or many can be entered)			
Case – Symptom fields	Have you travelled outside of NI in the 14 days before symptoms/test?	Manually selected by contact tracers	Yes or No
Case – Symptom fields	Countries Visited	Manually entered by contact tracers	If yes is selected to travel question above
Case – Symptom fields	Travel Information	Manually entered by contact tracers	
Case – Symptom fields	Health Advice Given	Manually selected by contact tracers	Yes or No
Case –Close Contact Information (one or many can be entered)	Close Contact First Name	Manually entered by contact tracers	Completed per close contact details provided by Contact
Case –Close Contact Information (one or many can be entered)	Close Contact Last Name	Manually entered by contact tracers	Completed per close contact details provided by Contact
Case –Close Contact Information (one or many can be entered)	Close Contact Gender	Manually entered by contact tracers	Completed per close contact details provided by Contact
Case –Close Contact Information (one or many can be entered)	Close Contact Telephone Number	Manually entered by contact tracers	Completed per close contact details provided by Contact
Case –Close Contact Information (one or many can be entered)	Close Contact Email	Manually entered by contact tracers	Completed per close contact details provided by Contact
Case –Close Contact Information (one or many can be entered)	Close Contact Alternative Contact Name	Manually entered by contact tracers	Completed per close contact details provided by Contact
Case –Close Contact Information (one or many can be entered)	Close Contact Alternative Contact Number	Manually entered by contact tracers	Completed per close contact details provided by Contact

Case –Close Contact Information (one or many can be entered)	Work in healthcare	Manually selected by contact tracers	Yes or No; Completed per close contact details provided by Contact
Case –Close Contact Information (one or many can be entered)	Type of Contact	Manually selected by contact tracers	Close contact, non close contact or complex contact; Completed per close contact details provided by Contact
Case–Close Contact Information (one or many can be entered)	Date of Last Contact	Manually entered by contact tracers	Completed per close contact details provided by Contact
Case–Close Contact Information (one or many can be entered)	Contact Setting	Manually selected by contact tracers	Healthcare, Household, Social, Travel, Work or Other; Completed per close contact details provided by Contact
Case–Close Contact Information (one or many can be entered)	Under 16	Manually selected by contact tracers	Yes or No; Completed per close contact details provided by Contact
Case–Close Contact Information (one or many can be entered)	Have they been unwell since you last saw them	Manually selected by contact tracers	Yes or No; Completed per close contact details provided by Contact
Case–Close Contact Information (one or many can be entered)	Close Contact Address line 1	Manually entered by contact tracers	Completed per close contact details provided by Contact
Case–Close Contact Information (one or many can be entered)	Close Contact Address line 2	Manually entered by contact tracers	Completed per close contact details provided by Contact
Case–Close Contact Information (one or many can be entered)	Close Contact Address line 3	Manually entered by contact tracers	Completed per close contact details provided by Contact
Case–Close Contact Information (one or many can be entered)	Close Contact City	Manually entered by contact tracers	Completed per close contact details provided by Contact
Case–Close Contact Information	Close Contact County	Manually entered by contact tracers	Completed per close contact details provided by Contact

(one or many can be entered)			
Case –Close Contact Information (one or many can be entered)	Close Contact Postcode	Manually entered by contact tracers	Completed per close contact details provided by Contact

Digital Self Trace Data

Area	Field Title	Primary Data Source	Corresponding data field in MS Dynamics
Case – Procedural field	Test ID	Provided by SMS message and manually entered by citizen	Test ID, used as the matching criteria
Case – Demographics fields	Surname	Manually entered by citizen	Surname
Case – Demographics fields	First name	Manually entered by citizen	First name
Case – Demographics fields	Age	Manually selected by citizen	Age
Case – Demographics fields	Postcode	Manually entered by citizen	Postcode
Case – Demographics fields	Contact Telephone Number	Manually entered by citizen	Primary Contact Number
Case – Demographics fields	Ethnic Group	Manually selected by citizen	Ethnic Group
Case – Employment fields	Type of Employment	Manually selected by citizen	Healthcare Worker
Case – Employment fields	Employer Name	Manually entered by citizen	Employer Name
Case – Employment fields	Employer Contact Number	Manually entered by citizen	Employer Contact Number
Case – Employment fields	Been @ work in last 7 days (Y/N) ?	Manually selected by citizen	Been in work
Case – Symptom fields	Symptomatic (Y/N)	Manually selected by citizen	Symptomatic

Case – Symptom fields	Self-Isolating (Y/N) ?	Manually selected by citizen	Isolation behaviour
Case – Symptom fields	Have you travelled outside of NI in the 14 days before symptoms/test (Y/N)?	Manually selected by citizen	Have you travelled outside of NI in the 14 days before symptoms/test
Case –Close Contact Information (one or many can be entered)	Contact type	Manually selected by citizen	Contact type
Case –Close Contact Information (one or many can be entered)	Close Contact Name	Manually entered by citizen	Close Contact First Name Close Contact Last Name
Case –Close Contact Information (one or many can be entered)	Close Contact Telephone Number	Manually entered by citizen	Close Contact Telephone Number
Case –Close Contact Information (one or many can be entered)	Close Contact Postcode	Manually entered by citizen	Close Contact Postcode
Case –Close Contact Information (one or many can be entered)	Work in healthcare (Y/N)?	Manually selected by citizen	Work in healthcare ?
Case –Close Contact Information (one or many can be entered)	Under 16 (Y/N)?	Manually selected by citizen	Under 16 ?

Data verified/collected from close contact (referred to as Call 2)

Area	Field Title	Primary Data Source	Additional Information
Close Contact – Procedural fields	Status	Manually entered by contact tracers	Open, In progress, closed
Close Contact – Procedural fields	Outcome	Manually entered by contact tracers	Successful/unsuccessful
Close Contact – Procedural fields	Outcome – unsuccessful reason	Manually entered by contact tracers	Eg Tried 5 times within 48 hrs, Case episode duplicated etc
Close Contact – Procedural fields	Date of call	Manually entered by contact tracers	
Close Contact – Procedural fields	Call attempt number	Manually selected by contact tracers	
Close Contact – Procedural fields	Timeline Title	Manually entered by contact tracers	Used by contact tracers to record call attempts details eg contact asked to be contacted tomorrow morning
Close Contact – Demographics fields	First Name	Provided by contact	Verified by contact tracer and updated if required
Close Contact – Demographics fields	Last Name	Provided by contact	Verified by contact tracer and updated if required
Close Contact – Demographics fields	Phone Number	Provided by contact	Verified by contact tracer and updated if required
Close Contact – Demographics fields	Gender	Provided by contact	Verified by contact tracer and updated if required
Close Contact – Demographics fields	Email	Provided by contact	Verified by contact tracer and updated if required
Close Contact – Demographics fields	Address line 1	Manually entered by contact tracers	Verified by contact tracer and updated if required
Close Contact – Demographics fields	Address line 2	Manually entered by contact tracers	Verified by contact tracer and updated if required
Close Contact – Demographics fields	Address line 3	Manually entered by contact tracers	Verified by contact tracer and updated if required
Close Contact – Demographics fields	City	Manually entered by contact tracers	Verified by contact tracer and updated if required

Close Contact – Demographics fields	County	Manually entered by contact tracers	Verified by contact tracer and updated if required
Close Contact – Demographics fields	Postcode	Manually entered by contact tracers	Verified by contact tracer and updated if required
Close Contact – Demographics fields	Under 16	Provided by contact	Verified by contact tracer and updated if required
Close Contact – Demographics fields	Close contact Deceased?	Manually selected by contact tracers	Yes or No
Close Contact – Demographics fields	Date of Death	Manually entered by contact tracers	If Close contact deceased is set to Yes
Close Contact – Demographics fields	Well enough to speak?	Manually selected by contact tracers	Yes or No
Close Contact Proxy Details (only populated if required)	Proxy Reason	Manually selected by contact tracers	
Close Contact Proxy Details (only populated if required)	Proxy First name	Manually entered by contact tracers	
Close Contact Proxy Details (only populated if required)	Proxy Last name	Manually entered by contact tracers	
Close Contact Proxy Details (only populated if required)	Proxy contact number	Manually entered by contact tracers	
Close Contact – Symptom fields	Symptomatic?	Manually selected by contact tracers	Yes or No
Close Contact – Symptom fields	Date of Onset	Manually entered by contact tracers	If Symptomatic is set to Yes
Close Contact – Symptom fields	Test for COVID?	Manually selected by contact tracers	Yes or No
Close Contact – Symptom fields	Test result options	Manually selected by contact tracers	Positive, Negative or No Result; if test for COVID is set to Yes
Close Contact – Symptom fields	Self-isolating?	Manually selected by contact tracers	Yes or No
Close Contact – Symptom fields	Isolation start date	Manually entered by contact tracers	
Close Contact – Symptom fields	Isolation end date	Manually entered by contact tracers	

Close Contact – Symptom fields	Recent Overseas Travel?	Manually selected by contact tracers	Yes or No
Close Contact – Symptom fields	Details of Travel	Manually entered by contact tracers	If Recent travel is set to Yes
Close Contact – Symptom fields	Already contacted by CTC?	Manually selected by contact tracers	Yes or No
Close Contact – Symptom fields	Fever/High Temp	Manually selected by contact tracers	Yes or No
Close Contact – Symptom fields	New persistent cough	Manually selected by contact tracers	Yes or No
Close Contact – Symptom fields	Shortness of Breath	Manually selected by contact tracers	Yes or No
Close Contact – Symptom fields	Loss of sense of smell	Manually selected by contact tracers	Yes or No
Close Contact – Symptom fields	Health Advice Given	Manually selected by contact tracers	Yes or No

Please note manually entered by contact tracers will be based upon the information provided by the contact (positive case citizen) or contacts proxy[2] and close contact or close contact proxy during dialogue with a contact tracer.

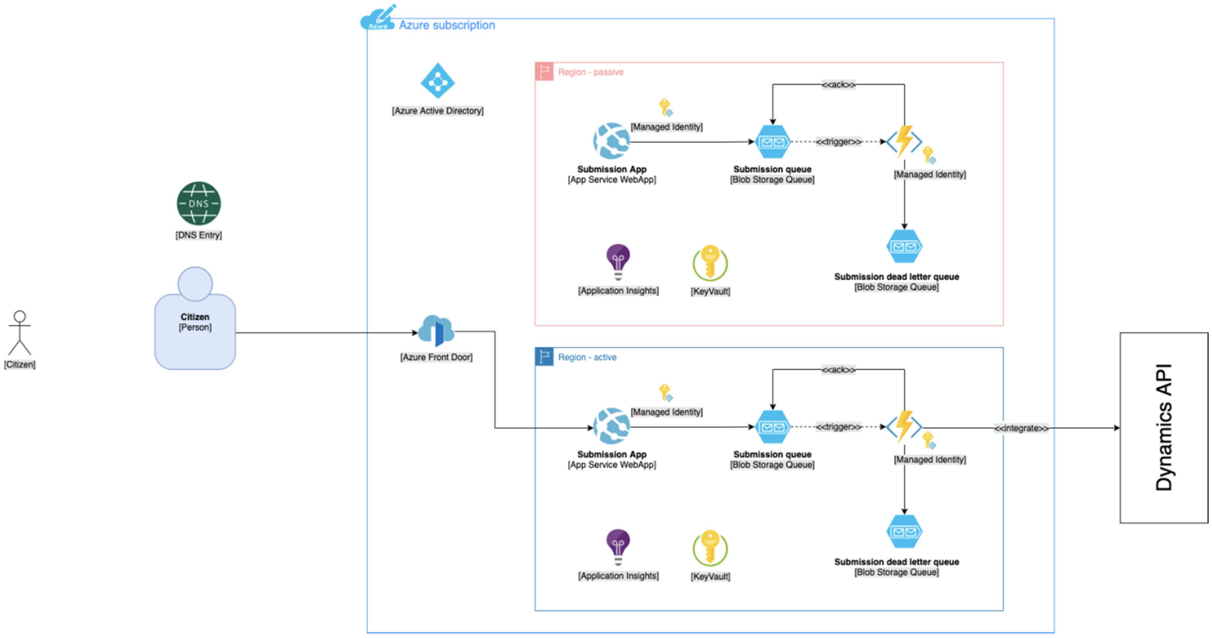
[2] 'Proxy' is where someone else speaks on behalf of an individual, for example a parent/guardian for a child under 16 years of age; where a person is unable to speak or understand English etc.

5.3 Data Storage and Transfer

The Central test registry resides within HSC Business Services Organisation (BSO) Information Technology Service (ITS) and is held on the BSO data centres. The Data extract is automatically generated within the Central Test Registry and then transferred via File Transfer Protocol (FTP). File Transfer Protocol is a standard network protocol used for the transfer of computer files between a client and server on a computer network. The transfer location is a dedicated folder within the existing PHA shared drive. Access is restricted by BSO ITS and any changes must be approved by PHA.

Only identified users within the contact tracing service have the correct access rights to trigger the data import. The allocation of these access rights are controlled by PHA. Only PHA identified and approved staff have access to the 'live' environment (containing personal data). Access to the environments have been added to the main "HSCNI.net" domain. All support services accounts (Kainos) have been set up by BSO to administer the environment.

Digital Self Trace web application resides on Belfast Health and Social Care secure cloud infrastructure.

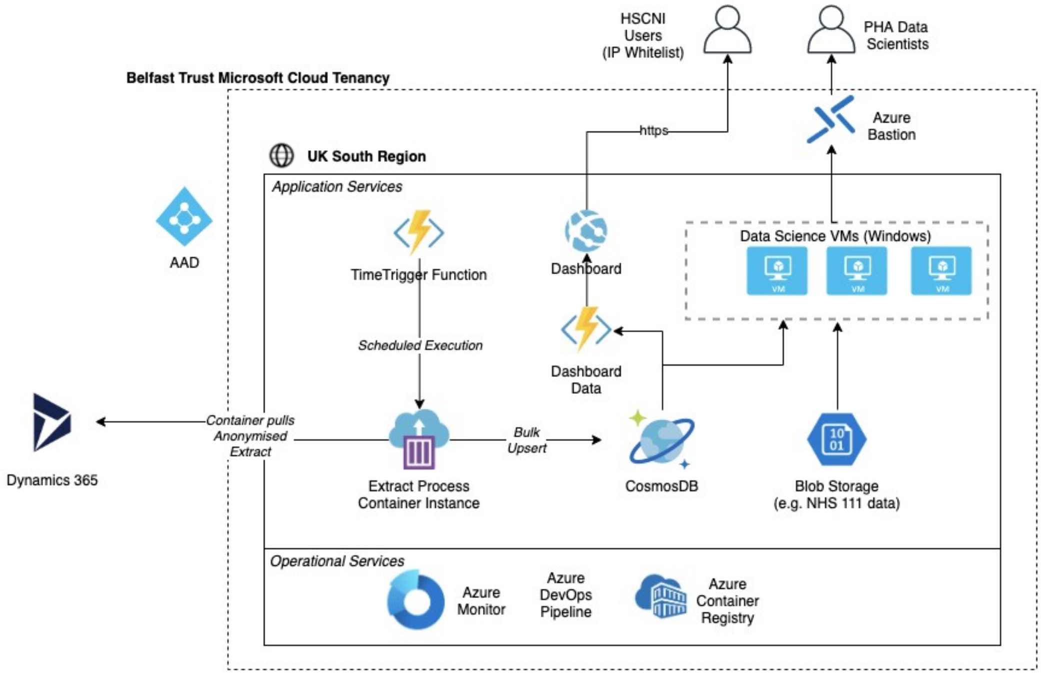


The web application itself is accessed via a web browser and the citizen types in their data. All data is stored in the browser cache while being completed (see Appendix L for cookie policy) and no data is transmitted until the final page is reached and the submission button is clicked.

At this point the data is transmitted as a JSON data payload with TLS encryption to Microsoft Azure. Here it is placed in a submission queue from which is it submitted to CTIS via the API. The use of the queue is to ensure handling of high usage volumes to restrict its impact on CTIS. All data is encrypted in transit and at rest.

There is only one instance of the data and it is not replicated, the data flows through the journey outlined above and is not retained on DST.

Analytic Platform resides on Belfast Health and Social Care secure cloud infrastructure.



The analytics function transfers a named patient copy of the CTS data field information onto a separate Microsoft database (Cosmos DB). There is a staggered upload of the data from Ms Dynamics every hour into the database. This is to ensure the data is up to date but that there is no service decrease with MS Dynamics due to resource usage; essentially acting as a typical reporting environment. The data is held securely within a multiple authenticated, GDPR compliant Microsoft platform. The information is hosted in this single secure environment which can be analysed, as required, to enable an appropriate response to this pandemic.

Identified and approved users have access to run specific queries on datasets. Users access the data via assigned dedicated virtual machines (VM). The VM will take the data temporarily and once the query is finished it will return the data. Data does not leave the Cosmo DB database, no data can be downloaded onto another system – access is granted on a performed function basis and automatically audited.

The analytic platform uses personal identifiable data to produce business dashboards that display anomysied data. These dashboards are used by the PHA and can be shared with DOH if necessary.

5.4 Data Retention

The personal data will only be held for as long as necessary in line with the PHA Retention and Disposal Schedule (Good Management, Good Records) and specific guidance issued by the Department of Health in Northern Ireland. Good Management, Good Records (GMGR) is the DoH retention and disposal schedule, that all HSC organisations in NI are required to comply to.

While contact tracing records are not specifically referenced in GMGR, the most relevant schedule is Disposal Schedule Section G Part 2 (G86) (https://www.health-ni.gov.uk/articles/disposal-schedule-section-g-part-2) This means that we will keep the personal data held within the contact tracing service for a period of 8 years.

This retention period is currently under further consideration, and this DPIA will be updated as soon as the timescale is confirmed. It is suggested that a differentiation be made between records relating to confirmed cases and those relating to their contacts. The proposed retention and disposal schedule would hold personal data on confirmed cases initially for a period of 4 years, when the retention period will be reviewed, with the possibility to hold the data for a further 4 years (i.e. a maximum of 8 years). Data on contacts would be held for 2 years, when the retention period will be reviewed, with the potential to hold for a further 2 years (maximum of 4 years).

As this is a divergence from GMGR approval is currently being sought from the DoH.

Personal data is held for this period for the purposes of studying potential re-infection, look back investigations or for legal purposes. This is particularly important as COVID 19 is a new disease, and there is still significant uncertainty about how it will progress, immunity (and how long any immunity will last) and on what impact it may have on individuals in future years. The data held in the PHA contact tracing service will be the single source of data relating to confirmed cases of COVID 19 and their contacts, and will be essential where it is necessary to track back an individual and their contacts for clinical purposes, enabling longitudinal studies (being able to link cases and follow people up) and to learn from outbreaks.

Anonymised data, for the purposes of further analysis, planning and trends, may be kept for longer.

5.5 Data transferred out from the PHA Contact Tracing Service

Some personal data may be shared with the GP of the person who has tested positive or the GP of a contact. This will be via a referral from a doctor in the PHA CTS to the GP, and would be done with the consent of the individual. However on rare occasions it may be necessary to do this in the absence of consent, for example if the individual took ill or collapsed during the phone call.

Personal data may be shared with the responsible public health bodies in Wales/Scotland/England/Republic of Ireland (or any other country where relevant) where the confirmed case has visited that country or been in contact with someone who lives in that country during the period when they have been potentially infectious. The information would be used so that the relevant Health Protection service could make contact and provide the appropriate advice to protect the individual and help prevent further spread of the virus.

The process for this is as follows:
Where the confirmed case provides details of one or more contacts who live in the Republic of Ireland (RoI), England, Scotland or Wales, the details of the contacts will be sent to the appropriate local Health Protection Team. (The PHA Health Protection Team holds the contact details for the Health Protection Teams in RoI, England, Scotland and Wales.) The information will be handed over via a telephone call from one registered health professional to another. In the event that a large number of contacts have been identified a document containing the information will be sent via an encrypted email.

Where the confirmed case resides in RoI, England, Scotland or Wales with contacts identified as residing in Northern Ireland, the process would work in reverse, with contact details provided to the PHA Contact Tracing Service to follow up in NI.

The Minimum Data Set:
Administrative details for those providing the information (name, organisation, position, contact details);
Personal data relating to case/contacts of confirmed COVID 19 cases –

- First name;
- Second name;
- Address (including postcode);
- Date of Birth (where available);
- Contact telephone number

Details of the confirmed case would not normally be shared. However, following risk assessment by the relevant health professionals, this may be deemed necessary. If the details of the confirmed case are to be shared with the health professionals in the receiving jurisdiction, the individual (‘confirmed case’) will be informed, and their information will be shared with their consent. The details of the confirmed case will not be shared with the contacts.

Data is currently shared with other jurisdictions in line with the International Health Regulations (2005) Part VIII, *Article 45, Treatment of Personal Data*. An MOU was agreed with the RoI to provide additional assurance on the continued sharing of health protection data in the event of a no deal EU Exit. Work is currently underway to reinforce these arrangements through specific data sharing agreements relating to COVID 19. In particular this will provide further reassurance regarding these data flows from 1 January 2021 when the UK leaves the EU.

Non identifiable data may be shared with Public Health England (PHE) for the purposes of UK national disease surveillance. It may also be shared with other relevant bodies, such as DoH (NI), universities or research bodies for the purposes of further analysis, planning and research into coronavirus.

5.6 SMS Messages from the PHA Contact Tracing Service

5.6.1 PECR

Both SMS are providing service information there is no marketing (neither SMS promotes the aims or ideals of the PHA or CTS).

5.6.2 SMS Message to Positive Cases

Once a new confirmed case (NI resident who has tested positive for COVID 19) has been loaded onto CTIS it will trigger an SMS message, from HSCtracing, inviting the citizen to complete Digital Self Trace (DST).

Dear ((firstName)) ((lastName))
You recently tested positive for COVID-19.

Please self-isolate.

We now need your help to trace your contacts.
Please use the Digital Self-Trace service: trace.covid-19.hscni.net
Use DST code: ((uniqueID)) (one time use)

5.6.3 SMS Message to Close Contacts

When PHA CTS close the data collection for the positive case they trigger an automated process sending all contacts, for that case, a SMS message. The SMS below is sent from HSCtracing and is addressed (firstname, surname) to the contact:

Dear ((firstName)) ((lastName))

You have been in close contact with someone who has COVID-19.

You are at high risk of having and spreading it. Self-isolate now for x days.

For more guidance visit covid-19.hscni.net/closecontact/

National Cyber Security Centre provided guidance on both the name of the service and contents of text messages; both of which have been classed as technically suitable for use

6. Consultation

The Contact Tracing Service is being established under the strategic direction of an Oversight Group chaired by the DoH Chief Medical Officer (CMO); and a Contact Tracing Steering Group established by the CMO. The Steering Group, which reports to the CMO, is independently chaired by Dr L Mitchel and Mr A Findlay with membership from DoH, PHA, PCC, NICVA and other stakeholders.

Key stakeholders include:

- The Northern Ireland public
- Department of Health
- Public Health Agency
- Public Health Agency Data Protection Officer (DPO)
- Health and Social Care Board
- Health and Social Care Trusts
- Business Services Organisation – (HR, DLS, IT)
- Queens & Ulster Universities
- Kainos – software development company and provider of some digital platforms
- NI Direct – call centre provider
- Political representatives
- Media
- Interest groups (human rights, privacy, women's rights, older people, children, minority ethnic, disability groups etc).
- Information Commissioners Office

Due to the urgent requirement to establish and operationalise the service, a formal consultation was not undertaken. However, informal engagement is ongoing with a range of stakeholders.

The Steering Group has engaged directly with NI Commissioners for Children & Young People; Older People; Equality; & Human Rights and the Information Commissioners Office in the course of its work.

The Programme Director, a medical consultant and the Chief Digital Information Officer have held engagement events facilitated by the PHA Comms team. Remote (video conference) sessions have been held with members of the Health Committee; a selection of Human Rights interest groups; and Trade Unions. Following these sessions, additional questions and comments have been received and responded to in respect of the Contact Tracing service. Stakeholders have mainly been interested in the staffing model to be adopted, the contact tracing methodology, the proximity app and the use of information.

The Chief Executives of the Patient and Client Council (PCC) and NICVA are members of the Steering Group and present views from the perspective of the service user on various issues.

Additionally, research has been undertaken by Big Motive on various aspects of contact tracing and the public perception thereof. (See appendix G)

PHA also remains in close contact with our counterparts in England and the other devolved administrations as well as the Republic of Ireland in order to share learning.

The pilot phase of the programme has been evaluated and learning shared with appropriate stakeholders.

Programme leads have liaised extensively with the PHA DPO and BSO Directorate of Legal Services, taking account of advice and comments in developing this DPIA and ensuring that appropriate measures are in place to safeguard individual's personal data. There has also been significant engagement with the ICO office in NI.

Equality and rural needs screening/assessment are also being taken forward in parallel.

7. Necessity and Lawful Basis

Contact Tracing is an established and recognised methodology for controlling and reducing the spread of communicable infectious diseases, that is used nationally and internationally. The World Health Organisation states:

"Coronavirus disease 2019 (COVID-19) is caused by the SARS-CpV-2 virus, and spreads from person-to-person through droplet and contact transmission. To control the spread of COVID-19, interventions need to break the chains of human-to-human transmission, ensuring that the number of new cases generated by each confirmed case is maintained below 1 (effective reproduction number <1). As part of a comprehensive strategy, case identification, isolation, testing and care, and contact tracing and quarantine, are critical activities to reduce transmission and control the epidemic."

"Contact tracing is the process of identifying, assessing, and managing people who have been exposed to a disease to prevent onward transmission. When systematically applied, contact tracing will break the chains of transmission of an infectious disease and is thus an essential public health tool for controlling infectious disease outbreaks."

"When countries have passed the peak of transmission and case numbers are decreasing, and particularly when stringent public health and social measures are being adjusted, rapid identification of cases and contact tracing are critical to maintain low levels of transmission and rapidly identify and break new transmission chains"[3]

The WHO guidance sets out the steps in undertaking contact tracing, emphasising that it is essential for contact tracing to be conducted for all confirmed cases:

- Define contacts
- Identify contacts
- Inform contacts

It outlines key information that must be gathered, stating that it should be held on electronic information systems, enabling the data to be analysed.

The PHA is accountable to the Department of Health (DoH), which is responsible for developing policy, and associated legislation, allocating resources and determining priorities. The DoH is accountable through the Minister for Health to the NI Assembly. The DoH published the policy document "COVID-19 Test, Trace and Protect Strategy – Saving lives by minimising SARS-CoV2 transmission in the community in Northern Ireland' 27

[3] Contact tracing in the context of COVID-19 Interim Guidance 10 May 2020 – World Health Organisation https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-COVID-19

May 2020. (https://www.health-ni.gov.uk/publications/COVID-19-test-trace-protect-support-strategy) The document sets out that contact tracing ("tracing of close contacts of cases") is a key element in the Department's strategy to minimise the spread of COVID 19, with the crucial aim of saving lives. The document sets out that the PHA has well-established experience and expertise in delivering contact tracing.
The DoH Chief Medical Officer (CMO) subsequently wrote to all HSC organisations informing them of this Strategy (HSC (MD) 38/2020 (https://www.health-ni.gov.uk/sites/default/files/publications/health/HSS%28MD%29-38-2020.pdf)

Contact tracing is routinely used by the PHA Health Protection Team to manage a range of communicable diseases, in line with the PHA statutory duty, as stated in the Health and Social Care (Reform) Act (Northern Ireland) 2009, which sets out the functions of the PHA, including that:
"*The health protection functions are the protection of the community (or any part of the community) against communicable disease in particular by the prevention or control of such disease*" (paragraph 13 (3)) (https://www.legislation.gov.uk/nia/2009/1/contents)

The PHA responsibilities in respect of health protection are also governed by the Public Health Act (Northern Ireland) 1967

The 'manual' contact tracing service, and associated Digital Self Trace, operated by the PHA, is the central element of the contact tracing programme, as it is essential to make personal contact with people to ensure that they have the knowledge and understanding of the implications of being a 'contact' and the actions that they need to take as a result. The information is also vital to map and manage clusters, informing decisions about further community interventions that may be necessary to limit the further spread of the disease.

The manual contact tracing service is supported by the 'Stop COVID NI' app, which uses anonymous information to alert users of the app if they have been in contact with someone who has tested positive. This is particularly useful in instances where it is not possible for an individual to know who they have been in contact with, for example on public transport. However, it is recognised that not everyone has access to a suitable 'smart' phone, nor may be willing to download the app. The app therefore cannot replace the personal contact tracing approach. (A separate DPIA for STOPCOVID19 has been developed by the DoH)

The manual contact tracing service will also be supported by the digital self-trace platform, which will allow individuals to provide details of their contacts digitally.

Only the minimum data set is processed, to enable 'confirmed cases' and their contacts to be identified, and to provide demographic data to identify and manage clusters and for public health surveillance – in line with established contact tracing methodology and based upon the Caldicott Principles. Contact tracing relies on identifying connections between people (person, place and time) and using that information to break potential chains of infection. There is no alternative at present to a skilled and experienced tracer using this information to make calls to those who have tested positive for COVID 19 and their contacts.

The COVID 19 contact tracing service has been established with the sole purpose of controlling and minimising the spread of COVID 19, to help save lives and help reduce pressure on the wider HSC system as a result of positive cases of COVID 19. COVID 19 is still a new and relatively unknown disease, and actions will be determined by both local (NI) experience of it as well as from wider national and international experience, knowledge and understanding. While it is recognised that specific actions may need to change, and may do so rapidly, as understanding and knowledge of the disease develops, the personal data collected through the COVID 19 contact tracing service will only be used for purposes of contact tracing (including cluster management) and public health surveillance in respect of COVID 19.

The contact tracing service sits within the governance structures of the PHA (the Agency Management Team and the PHA Board), and to the DoH via the Contact Tracing Steering Group and the DoH Test Trace and Protect Oversight Board.

7.1 Lawful Basis for Processing

The lawful basis for processing this personal information (i.e. personal data collected as part of the contact tracing service) according to the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 is:
GDPR Article 6(1)(e) - the processing is necessary for the performance of the Public Health Agency's official tasks carried out in the public interest.

The official functions of the Public Health Agency are set out in the Health and Social Care (Reform) Act (Northern Ireland) 2009. https://www.legislation.gov.uk/nia/2009/1/contents

The 2009 Act sets out the PHA health Protection function, including that "*The health protection functions are the protection of the community (or any part of the community) against communicable disease in particular by the prevention or control of such disease*". In respect of COVID 19, this means that the PHA will operate the Contact Tracing Service to help break the chain of transmission of the virus, as required by the Department of Health, in line with the DoH 'COVID-19 Test, Trace and Protect Strategy: Saving lives by minimising SARS-CoV2 transmission in the community in Northern Ireland', 27 May 2020. (https://www.health-ni.gov.uk/publications/COVID-19-test-trace-protect-support-strategy)

By identifying people who have been in close contact with someone who has tested positive for coronavirus, and then asking them to self-isolate we can limit the spread of the virus and minimise the risk of a second wave of infection, helping the move to more normal social and economic lives. This will also help to protect the Health Service from being overwhelmed.

Contact tracing is an established and recognised measure to control and reduce the spread of communicable diseases, internationally, as determined by the World Health Organisation (WHO). It is the only way of identifying individuals who have been in contact with someone who has tested positive for COVID 19, and providing them with advice on the actions that they should do to prevent further spread, and advice on what to do should they develop symptoms. While the STOPCOVIDNI app is also being used in NI to help ensure that people are aware of any contact with someone who has tested positive, it will not have universal coverage (eg all members of the public will not download it, may not have a smart phone, or may not have a smart phone that is compatible). Additionally, personal communication that can provide reassurance and help answer queries and concerns, is most effective in ensuring compliance with the need to self-isolate at the same time as providing assurance and assistance.

The information from contact tracing is also essential for managing and controlling clusters; this would not be possible without the collection of personal data to identify time, place and person. The analytics platform enables the real-time analysis of this data to quickly identify clusters and particular issues of concern, to enable targeted actions to be taken to help control and prevent the further spread of the virus.

The data collected by the Contact Tracing Service includes personal data. Some of this data relates to health data which is described as ‘special category data’.

GDPR Article 9(2) (i) – applies to this processing, that is, the processing is necessary for reasons of public interest in the area of public health.

Data Protection Act 2018 – Schedule 1, Part 1 (3) – reasons of public interest in the area of public health:

“This condition is met if the processing—

> *(a) is necessary for reasons of public interest in the area of public health, and*
>
> *(b) is carried out—*
>
> > *(i) by or under the responsibility of a health professional, or*
> >
> > *(ii) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.*

7.2 Data Quality and Minimisation

As set out in section 5.2 data is collected from a number of different sources, including established HSC systems. Data accuracy will be maintained through contact tracers checking details on the contact tracing system and confirming with both the person who has tested positive and their contacts that the data held is accurate.

The data collected is the minimum necessary to enable 'confirmed cases' and their contacts to be identified, and to provide demographic data to identify and manage clusters and for public health surveillance – in line with established contact tracing methodology and based upon good information governance practice.

7.3 Privacy

Contact tracers check the identity of the confirmed cases when they call them. The answers are matched against the information sent with the positive test results. Contacts are asked to confirm their name to ensure it matches with the information given by the confirmed case. Scripts are kept under review and updated as required.

Where the confirmed case or contact is under the age of 16; or cannot (for reasons of illness or infirmity); or prefers not to speak directly to the tracer; they are asked for permission to speak to a proxy. (In the case of a child under the age of 16 this is their parent or legal guardian. For those who have capacity but would like us to speak to a nominated proxy, this will be advised by the individual. If they lack capacity this would normally be their next of kin)

The confirmed case is never identified to the contact – although we acknowledge that they may be identifiable due to the circumstantial information provided and the fact that most contacts are in the same household as the confirmed case. Participation in the process is strongly encouraged but not mandated and if a confirmed case or a contact advises that they do not wish to proceed, the contact tracer will accept this decision and end the call. However, data on the test result will be retained on the contact tracing information system, along with a record that they were contacted and did not wish to participate. This information is needed as a record that they were contacted and, additionally, in case that they may test positive again as this may influence interpretation of the result and subsequent advice.

The PHA Contact Tracing Centre operates from a base in County Hall, Ballymena. Staff are employed by the PHA and as such must complete mandatory training – including in information governance awareness and information security.

Information on the use of information – including the Privacy Notice – is published on the PHA website, at: https://www.publichealth.hscni.net/COVID-19-coronavirus/testing-and-tracing-COVID-19/privacy-information

7.4 Data Protection Principles

The contact tracing service, including the contact tracing information system and digital self-trace, has been set up in line with the 7 data protection principles:

- There is a clear lawful purpose for collection of the data (see section on 'lawful basis for processing). The processing is fair and transparent in that personal data is only used for the specific purpose of contact tracing, cluster management and surveillance purposes to inform the control and management of COVID 19. Significant public information is being provided by CTS through a range of media channels as well as PHA website, so that the public are aware of the Service and how it may relate to them. The privacy notice relating to the CTS is also published on the PHA website, providing information on how their personal data is processed.
- The data collected for the contact tracing service will not be used for any purpose that is not linked to COVID 19.
- The data collected has been identified to ensure that it is adequate for the purpose of contact tracing, cluster management and health protection surveillance, but is not asking for anything that is not required for this purpose.
- Processes have been put in place to ensure the accuracy of data, as far as is reasonably possible, and to enable data to be corrected where appropriate.
- The data will be retained for a specified period, as described in this DPIA (recognising that the retention period is under review, with DoH approval being sought to vary from Good Management Good Records).
- Security measures are in place to protect the integrity and confidentiality of data.
- Governance and accountability arrangements are in place through the development of this DPIA and compliance with existing PHA governance and information governance arrangements, including information governance policies and procedures.

7.5 Data Rights

The GDPR sets out the 8 rights that individuals have in respect of their data. These have been considered in respect of the Contact Tracing Service as follows:

1. The right to be informed

Individuals are provided with information about the collection and use of their personal data for the CTS, including what personal data is collected, the purposes for collecting, retention periods and potential sharing of data. The information is available in the privacy notices published on the PHA website. In addition the PHA website also includes a range of information about the CTS, so that the public are informed and aware about the service and its importance in helping to control and reduce the spread of COVID 19 and therefore protect the health of individuals and the wider public.

2. Right of access

Individuals can ask for copies of the information that we hold about them. The PHA has an established subject access request (SAR) process to ensure that requests are dealt with promptly and appropriately.

3. Right to rectification

Individuals can ask to have inaccurate personal data corrected or completed if it is incomplete. CTS staff will verify data held during their calls with positive cases and their close contacts, as the accuracy of data is important for the effectiveness of the service. Individuals can also contact the PHA (in writing or verbally) to request that inaccurate data be rectified.

4. Right to erasure

GDPR introduced a right for individuals to have personal data erased ('the right to be forgotten'), however the right is not absolute and only applies in certain circumstances. In respect of the CTS, data held and processed includes information on positive tests received from the Central Testing Registry, and is necessary for contacting individuals to give advice (including self-isolation to reduce the spread of infection), identifying links, managing clusters and public health surveillance. Individual requests will be considered by the DPO with the Health Protection Consultants and discussed with the requester.

5. Right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data, however the right is not absolute. While individuals can request that the CTS stops processing their data, as set out in number 4 above, the data held will still need to be processed for the purpose of public health protection. However, while people are strongly encouraged to co-operate with the CTS and provide the additional information requested by the contact tracers, this is not mandatory.

6. Right to data portability

Individuals can ask the Contact Tracing Service to share their information with another organisation (although this may not always be possible). It should also be noted that individuals who have tested positive, following a test booked through the national testing initiative, will also receive their test result separately and directly.

7. Right to object

Individuals have the right to object to the processing of their personal data, including when the lawful basis for processing is public task. However, this is not an absolute right, and processing can continue if there are compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual. In the case of the CTS, the data is used for the overriding public interest to protect the health of the public through controlling and reducing the transmission of COVID 19.

8. Rights relating to automated decision making including profiling

While the CTS uses computer systems to process personal data, it does not include automated individual decision-making (i.e. making a decision solely by automated means without any human involvement).

The analytic platform does not use any automated processed at present rather it identifies statistical observation that are flagged to human being.

Every person added to Digital Self trace will get a notification (provided their details are accurately added) there is no algorithm determining the decision.

Digital Self Trace invitation SMS message will only be sent to over 16's, this is based on the DOB included in that CTIS receives from the central test registry not algorithm based.

Close contact alert SMS message will only be sent to those that the positive case has identified (verbally or via DST) this is also not algorithm based.

If an individual is not happy with what the contact tracing service does with the information that is held about them, they can contact the PHA DPO (details are provided in the privacy notice on the PHA website).

We are utilising some IT solutions to mitigate risks such as the transfer of personal data from the Central Test Registry (CTR) to the MS Dynamics system used to record information about index cases.

As set out in section 5.3, personal data may be shared with health protection teams in other UK jurisdictions or in the RoI. Data is only shared by health protection professional to health protection professional. Details are normally only shared about the contacts of a person who has tested positive who reside in the other jurisdiction, and only the minimum data set that is necessary to enable the health protection service in that jurisdiction to be able to contact them, and provide the advice that is relevant to that jurisdiction. In exceptional cases, where the Health Protection clinician makes a risk assessment that it is necessary to share the details of the person who tested positive, this will be done with the consent of the individual.

Work is currently underway to agree COVID 19 specific data sharing agreements, to provide further assurance, especially in respect of transfers with the RoI in the event of EU Exit.

The Contact Tracing Privacy Notice on the PHA website informs individuals that data may be shared with other jurisdictions.

7.6 Security Measures

Security measures are in place to ensure the information processed is carried out only as detailed in this DPIA and ultimately only for the purposes intended.

7.6.1 CTIS

The organisational security measures implemented include the following security controls that BSO have applied to the environment:

- Common data services is unavailable to everyone except for users within two Azure Active Directory groups
- Multi-Factor authentication is required to access the system outside of BSO Trusted locations (BSO Network).
- Legacy authentication has been blocked for all users.
- A user must have a Dynamic 365 license assigned before they are able to access Common data services.
- Users will not be able to use the system unless added to an application role.
- Application roles have been set up to ensure a “least privileged” approach (Kainos developed).
- Only required accounts have been sync’d from on premise to Azure Active Directory via AD Connect.

User access is only granted by an authorised PHA staff member liaising with a named contact in BSO ITS and completing a registration form. This is fully documented in an audit trail.

No live system access rights are allocated to 3rd parties. All 3rd party access is in accordance to agreed contacts and contract management processes.

An appropriate separation of roles will be employed, for example developers will manage supporting backend configurations, and the BSOs team will manage the central test registry.

7.6.2 DST

Digital Self Trace is not conceptually different from the process followed for manual contract tracing as the same back end system (Microsoft Dynamics) is used. The Digital Self Trace Web Application is simply an alternative data entry route.

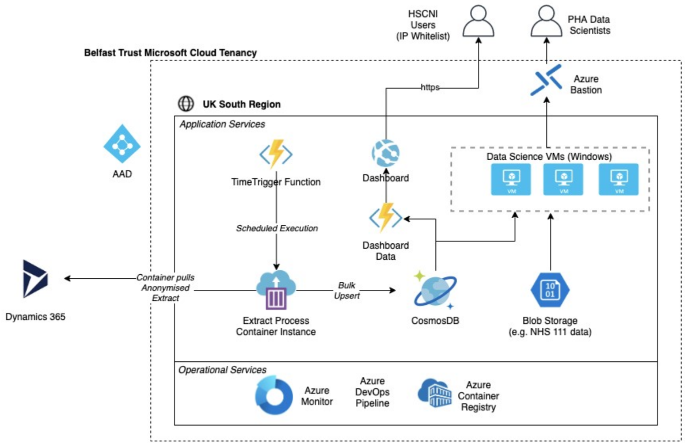
The Web application itself is accessed via a web browser using an unrestricted URL. The positive COVID-19 citizen (over 16 years old) enters their test code (from SMS Message) which is validated before they can enter details. All data is stored in the browser cache while being completed (see cookie policy, appendix L) and no data is transmitted until the final page is reached and the submission button is clicked.

At this point the data is transmitted as a JSON data payload with TLS encryption to Microsoft Azure. Here it is placed in a submission queue from which is it submitted to Dynamics via the API. The use of the queue is to ensure handling of high usage volumes to restrict its impact on CTIS. All data is encrypted in transit and at rest, see section 5.2 for architecture diagram.

External penetration testing has been completed on DST. The assessment included an assessment of web application and the associated source code. Full report has been received and remediation work has been carried out.

7.6.3 Analytics Platform

The organisational security measures implemented include the following security controls that have applied to the environment:



1. Restriction on user access:
    a. All Azure resources are managed via Azure Active Directory
    b. Access to Data Science Virtual Machines is restricted to via encrypted connection through Azure Bastion. Connection to Bastion is via whitelisted IP addresses only. Only named Azure Active Directory identities are allowed to access the DSVMs via this secure connection
    c. Access to the Analytics dashboard is currently whitelisted to only Kainos IP addresses. When planning to open this up to HSCNI staff, it will be to named individuals identified by Azure Active Directory identity and whitelisted to the appropriate HSCNI IP addresses only.

2. Security of data as it moves into and within the analytics platform:
    a. A named CRM service account with least-privilege access is used in conjunction with a registered Azure Active Directory App to authenticate and authorise the data extract application when connecting to the Contact Tracing system to retrieve data for sync to the analytics database
    b. This connection between the data extract application and Dynamics CRM web services is encrypted via SSL using TLS encryption

c. Connections to the Azure Cosmos DB database are also encrypted via SSL/TLS and access is only granted via managed identity used by the Data Science VMs, analytics dashboard and data extract processes. I.e. there is no direct access to the database via a user of the Azure portal
d. All data stored in Cosmos DB is encrypted at rest by default using AES-256 encryption. Ref: https://docs.microsoft.com/en-us/azure/cosmos-db/database-encryption-at-rest

7.6.4 Contact Tracing Staff

All staff are bound by HSCNI employment contracts which includes a clause on confidentially.

All contact training staff are required to complete a one day intensive course before system access is provided. This includes a dedicated session on data protection and information governance (developed with input from PHA Information Governance Manger). The training also includes supervised practice with the Education Lead. Training is delivered by a dedicated trainer (Education Lead) from the HSC Leadership Centre who has previous experience in delivering information governance training on behalf of the HSC (see appendix J).

All staff (including bank and honorary staff) must complete the regional HSC online information governance awareness and IT security training modules. (Or, if coming from another HSC organisation, have completed the training in the previous year).

7.7 Further Developments

As the pandemic develops the contact tracing service may have to change and develop accordingly. While it is impossible to predict these developments at this stage a number of developments are anticipated including:

- Consideration of how to collect details of contact tracing performed by HSC trusts in respect to COVID 19 exposure on their premises;
- Establishment of monitoring and quality assurance process. (One option includes call recording as standard and a bid has been made for funds to resource this);
- Agreement and sign off of MOU with the Home Office in relation to passenger locator forms (PLF);
- TTP analytics function uses cloud architecture, hosted within Microsoft UK Southern Region datacentres, using software already configured within the Belfast Trust. In the longer term it will ultimately be re-provisioned centrally within Business Services Organisation, when a Microsoft Azure environment for Northern Ireland can be constructed.

- New positive test results will be incorporated into existing feed from the Central Test Registry as new testing programs are rolled out eg LFT and LAMP.
- Consider of machine learning purposes, human element would remain. There is no automated decision made by machines in this process all decision are human made. There are no plans to change this in the future.

As the contract tracing service DPIA is a living document it will be updated as necessary.

8 Risks

Risks will be assessed using the both HSC regional risk matrix (Diagram C; full document in Appendix H)

	Impact (Consequence) Levels				
Likelihood Scoring Descriptors	**Insignificant(1)**	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Catastrophic (5)**
Almost Certain (5)	Medium	Medium	High	Extreme	Extreme
Likely (4)	Low	Medium	Medium	High	Extreme
Possible (3)	Low	Low	Medium	High	Extreme
Unlikely (2)	Low	Low	Medium	High	High
Rare (1)	Low	Low	Medium	High	High

8.1 Identification of Risks

#	Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Impact (consequence) of harm	Overall risk
1	Risk of inaccurate data (and potential contact with wrong people/missing correct people) through error in manual input of data into the Contact Tracing Information System or by citizen in Digital Self Trace. Potential impact of close contact not being contacted and associated risk of disease spread. Or cause unnecessary concern to people contacted in error.	Possible	Major	High
2	Risk of inaccurate data from labs which may have key information such as case details incorrect or missing meaning potential impact of a delay in contacting positive cases or positive case not being contacted and associated risk of disease spread. Or people with negative results being contacted in error and cause unnecessary concern.	Rare	Minor	Low
3	Risk of data loss during import which would result in inability to identify positive cases. Potential impact of positive cases not being contacted and associated risk of disease spread.	Possible	Minor	Low
4	Risk of inaccurate information from contact (deliberate or in error). Potential impact of close contact not being contacted and associated risk of disease spread (no self-isolation). Or unnecessary concern to people contacted in error and self-isolating without cause.	Possible	Moderate	Medium
5	Risk of not being able to contact contacts identified by the initial source. Potential impact of positive cases not being contacted and associated risk of disease spread (no self-isolation) along with the potential risk to their health.	Possible	Moderate	Medium

6	As this is a phone based system, communication issues - person may hear instructions/advice incorrectly and therefore may act contrary to the advice given (potential impact of no self-isolation and potential disease spread).	Possible	Moderate	Medium
7	Risk of data breach (with the loss or unauthorized sharing of personal identifiable data, with potential impact of distress or reputational damage to individuals.), by staff working in the contact Tracing Service and Health Protection Teams, through human error or intent. In addition the risk of reputational damage to the PHA.	Possible	Major	High
8	Risk of the CTIS being 'hacked', with the theft of personal identifiable data (data breach), with the risk of distress or reputational damage to individuals. Or the system being compromised or inaccessible as a result of a cyber security incident therefore contact tracing center being unable to operate with no positive cases or contacts being provided guidance on self-isolation etc. In addition the risk of reputational damage to the PHA.	Possible	Major	High
9	Risk of unauthorised access to the personal data on the CTIS, resulting in a data breach with potential impact of distress or reputational damage to individuals. In addition the risk of reputational damage to the PHA.	Possible	Major	High
10	Risk of unauthorised access (internal or external) to the personal data on the Analytic Platform, resulting in a data breach with potential impact of distress or reputational damage to individuals. In addition the risk of reputational damage to the PHA	Possible	Major	High
11	Risk relating to Child and Adult Safeguarding Privacy concerns, particularly regarding inappropriate access to current information on identity and location. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information. Communication issues with children/vulnerable adults – issues with	Possible	Major	High

	receiving/understanding information/instructions If there are inadequate disclosure controls, there is an increase in the likelihood of information being shared inappropriately			
12	Risk of noncompliance with PHA data protection and information governance policies and procedures which may result in accidental or deliberate misuse of sensitive personal data with potential of data protection requirements not being adhered to and for a data breach with the potential impact of distress or reputational damage to individuals. In addition the risk of reputational damage to the PHA.	Unlikely	Moderate	Medium
13	Risk of noncompliance with established BSO ITS Service Transition Approval Process (STAP). Potential, in error, to negatively impact the MS Dynamics environment and therefore the contact tracing information system would not be available (impacting on one tracer or entire contact tracing service user group)	Possible	Major	High
14	Risk of access to personal data by 3rd party processers which may result in accidental or deliberate use of sensitive personal information. Potential impact of a data breach, with potential impact of distress or reputational damage to individuals. In addition the risk of reputational damage to the PHA.	Unlikely	Major	High
15	Risk of complaints/legal action from someone contacted by the service who feels that their Human Rights have been violated in that it has identified them as being in a certain place, with a certain person/persons.	Possible	Moderate	Medium
16	Risk that robust data sharing arrangements will not be in place for international transfers resulting in an inability to share data in respect of contacts with other countries outside of the UK especially after EU Exit. Potential impact of close contacts not being contacted and associated risk of disease spread (no self-isolation).	Possible	Moderate	Medium
17	Risk that personal data is used inappropriately for analytical purposes.	Possible	Moderate	Medium

	Inappropriate sharing of personal data which could result in potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the PHA.			
18	Risk of fraudsters sending similar looking messages with malicious intent. Potential impact of distress or reputational damage to individuals, in addition the risk of reputational damage to the PHA.			
19	Risk of the DST being ‘hacked’, with the theft of personal identifiable data (data breach), with the risk of distress or reputational damage to individuals. Or the system being compromised or inaccessible as a result of a cyber security incident therefore contact tracing center being unable to operate with no positive cases or contacts being provided guidance on self-isolation etc. In addition the risk of reputational damage to the PHA.	Possible	Major	High
20	Risk of fraudsters setting up a similar webapp as Digital Self Trace with malicious intent. Potential impact of distress or reputational damage to individuals, in addition the risk of reputational damage to the PHA.	Possible	Moderate	Medium
21	SMS messaging failure could be missed by the system, meaning that positive COVID-19 citizens would not have a test code for use in DST.	Possible	Moderate	Medium

8.2 Measures to reduce risk

#	Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk
1	Risk of inaccurate data (and potential contact with wrong people/missing correct people) through error in manual input of data into the Contact Tracing Information System or by citizen in Digital Self Trace. Potential impact of close contact not being contacted and associated risk of disease spread. Or cause unnecessary concern to people contacted in error.	Automatic electronic transfer/upload of data from Central Test Registry to the Contact Tracing Information System. Automatic electronic transfer of data from Digital Self Trace to the Contact Tracing Information System. Verification of information by Contact Tracers with Confirmed Cases and Contacts during telephone calls. Supervision through the Contact Tracing Service Manager. A Quality Improvement (QI) initiative has commenced, which will include a focus on process/quality of training/quality of scripts/quality of calls. One option being explored includes call recording as standard and a bid has been made for funds to resource this. Training of staff (see Appendix J) and procedures clearly set out (including scripts for calls)	Reduced	Low
2	Risk of inaccurate data from labs. Potential impact of positive cases not being contacted and associated risk of disease spread. Or	All Lab data is provided by the automatic electronic transfer/upload of data	Maintained	Low

	people with negative results being contacted in error and cause unnecessary concern.	All essential data relating to the test is held within MS Dynamics (CTR ID and Test ID) so if a test has been withdrawn/replaced by Labs the required data is there to enable validation. Assurance from BSO ITS in respect to data quality of the central test registry (see appendix I)		
3	Risk of data loss during import. Potential impact of positive cases not being contacted and associated risk of disease spread.	Automatic electronic import process is used to load the CTR extract on the Contact Tracing Information System. Data is automatically submitted from Digital Self Trace on the Contact Tracing Information System. All records (CTR and DST) are loaded or rejected (requiring manual intervention) The CTR import file remains available, for a 7 day period, for additional review if necessary. After 7 days the file is auto deleted.	Reduced	Low
4	Risk of inaccurate information from contact (deliberate or in error). Potential impact of close contact not being contacted and associated risk of disease spread (no self-isolation). Or unnecessary concern to people contacted in error and self-isolating without cause.	Contact tracers are trained (see appendix J) and experienced so will take all possible steps to ensure contact is clear about what is being asked so can answer fully. Tracers can make a follow up call to the contact if they feel the contact requires additional time to process the questions. Digital Self Trace specifies what a close contact is to ensure the citizen understands. There is a large amount of material available via website, apps etc to ensure the public are fully	Reduced	Low

		aware of what information will be required and why. Public is encouraged to use the StopCOVID app which will automatically notify close contacts. Ongoing communications and engagement with key stakeholders emphasize the need to engage with the service in order to slow the spread of the disease.		
5	Risk of not being able to contact contacts identified by the initial source. Potential impact of positive cases not being contacted and associated risk of disease spread (no self-isolation).	Contact trackers use the information provided by the contact on close contacts. SMS is sent to contacts advising them to self-isolate, this is sent using the number supplied by the close contact (either verbally or DST). If this information is incorrect tracers can re-contact the contact and ask for more information if they can provide some. Tracers make five attempts to contact cases and close contacts. This has been increased from three (based on experience and learning). Public are encouraged to use the StopCOVID app which will automatically notify close contacts.	Reduced	Low
6	As this is a phone based system, communication issues - person may hear instructions/advice incorrectly and therefore may act contrary to the advice given (no self-isolation and potential disease spread).	Contact tracers are trained (see Appendix J)and experienced so will take all possible steps to ensure contact is clear about what is being asked so can answer fully. Tracers can make a follow up call to the contact if they feel the contact requires additional time to process the questions. If a tracer has a concern about the capacity of the contact they can refer the call	Reduced	Low

		across to the clinical lead. There is a large amount of material available via website, apps etc to ensure the public are fully aware of what information will be required and why.		
7	Risk of data breach (with the loss or unauthorized sharing of personal identifiable data, with potential impact of distress or reputational damage to individuals), by staff working in the contact Tracing Service and Health Protection Teams, through human error or intent. In addition the risk of reputational damage to the PHA.	All involved in the CTS are required to complete the HSC information governance and IT Security e learning module; Information Governance manager has provided data protection slides for incorporation and use in the training for call handlers; Information Governance manager has provided a data protection 'check list' for each work station. Supervision via the Contact Tracing Service Manager. A Quality Improvement (QI) initiative has commenced, which will include a focus on process/quality of training/quality of scripts/quality of calls. One option being explored includes call recording as standard and a bid has been made for funds to resource this. Risk and management of breach of confidentiality covered in training, in line with PHA Data Protection /Confidentiality Policy and Data Breach Incident Response Policy. Staff subject to regulatory Codes of Conduct eg NMC and GMC which include duties of confidentiality.	Reduced	**Medium**

		All HSC staff subject to HSC Code of Conduct. Confidentiality clauses in contracts of employment of PHA staff Appropriate disciplinary action will be taken in the event of proven breach		
8	Risk of the CTIS being 'hacked', with the theft of personal identifiable data (data breach), with the risk of distress or reputational damage to individuals. Or the system being compromised or inaccessible as a result of a cyber-security incident therefore contact tracing center being unable to operate with no positive cases or contacts being provided guidance on self-isolation etc. In addition the risk of reputational damage to the PHA.	Microsoft complies with both international and industry-specific compliance standards and participates in rigorous third-party audits that verify security controls. As required by the GDPR, Microsoft implements and maintains appropriate technical and organizational security measures, including measures that meet the requirements of ISO 27001 and ISO 27018, to protect personal data it processes as a data processor or sub processor on its customers' behalf. Microsoft follows the EU Standard Contractual Clauses (data resides in a secure cloud within the UK). BSO have applied the following security controls: ● Common data services is unavailable to everyone on WWW except for users within two Azure Active Directory groups ● Multi-Factor authentication is required to access the system outside of BSO Trusted locations (BSO Network). ● Legacy authentication has been blocked for all users. ●A user must have a Dynamic 365 license assigned before they are able to access Common	Reduced	**Medium**

		data services. ● Users will not be able to use the system unless added to an application role. ● Application roles have been set up to ensure a "least privileged" approach (Kainos developed). ● Only required accounts have been sync'd from on premise to Azure Active Directory via AD Connect.		
9	Risk of unauthorised access to the personal data on the CTIS, resulting in a data breach with potential impact of distress or reputational damage to individuals. In addition the risk of reputational damage to the PHA.	BSO have applied the following security controls to all environments including Live: ● Common data services is unavailable to everyone on WWW except for users within two Azure Active Directory groups ● Multi-Factor authentication is required to access the system outside of BSO Trusted locations (BSO Network). ● Legacy authentication has been blocked for all users. ●A user must have a Dynamic 365 license assigned before they are able to access Common data services. ● Users will not be able to use the system unless added to an application role. ● Application roles have been set up to ensure a "least privileged" approach (Kainos developed). ● Only required accounts have been sync'd from on premise to Azure Active Directory via AD Connect. User access is only granted by an authorised PHA	Reduced	**Low**

		staff member liaising with a named contact in BSO ITS and completing a registration form. This is fully documented in an audit trail. All staff bound by HSCNI employment contracts. A Quality Improvement (QI) initiative has commenced, which will include a focus on process/quality of training/quality of scripts/quality of calls. One option being explored includes call recording as standard and a bid has been made for funds to resource this.		
10	Risk of unauthorised access (internal or external) to the personal data on the Analytic Platform, resulting in a data breach with potential impact of distress or reputational damage to individuals. In addition the risk of reputational damage to the PHA.	● All Azure resources are managed via Azure Active Directory ● Access to Data Science Virtual Machines is restricted to via encrypted connection through Azure Bastion. Connection to Bastion is via whitelisted IP addresses only. Only named Azure Active Directory identities are allowed to access the DSVMs via this secure connection ● Access to the Analytics dashboard is currently whitelisted to only Kainos IP addresses. When planning to open this up to HSCNI staff, it will be to named individuals identified by Azure Active Directory identity and whitelisted to the appropriate HSCNI IP addresses only. ● Security of data as it moves into and within the analytics platform: ● A named CRM service account with least-privilege access is used in conjunction with a registered Azure Active Directory App to	Reduced	**Low**

		authenticate and authorise the data extract application when connecting to the Contact Tracing system to retrieve data for sync to the analytics database ● This connection between the data extract application and Dynamics CRM web services is encrypted via SSL using TLS encryption ● Connections to the Azure Cosmos DB database are also encrypted via SSL/TLS and access is only granted via managed identity used by the Data Science VMs, analytics dashboard and data extract processes. I.e. there is no direct access to the database via a user of the Azure portal ● All data stored in Cosmos DB is encrypted at rest by default using AES-256 encryption. Ref: https://docs.microsoft.com/en-us/azure/cosmos-db/database-encryption-at-rest All staff bound by HSCNI employment contracts.		
11	Risk relating to Child and Adult Safeguarding Privacy concerns, particularly regarding inappropriate access to current information on identity and location. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information. Communication issues with children/vulnerable adults – issues with receiving/understanding information/instructions	Access to the system is controlled (as set out above), so no unauthorised personnel have access to the CTIS. Only authorised Contact Tracing and Health Protection staff have access to the data on the CTIS; they are bound by the existing controls and policies and professional regulatory Codes of Conduct. CTS operated by staff recruited for their professional skills (eg nursing) that will assist in	Reduced	Medium

	If there are inadequate disclosure controls, there is an increase in the likelihood of information being shared inappropriately	communicating with children and vulnerable adults. In respect of children and vulnerable adults the contact tracers will seek to speak to a proxy (eg children would be parent or legal guardian). If a tracer has a concern about the capacity of the contact they can refer the call across to the clinical lead. Managerial and clinical supervision arrangements in place via the Contact Tracing Service Manager and the Clinical Lead. Legal advice is sought as required		
12	Risk of noncompliance with PHA data protection and information governance policies and procedures resulting in data protection requirements not being adhered to and potential for data breach with the potential impact of distress or reputational damage to individuals. In addition the risk of reputational damage to the PHA.	Development of DPIA to identify risks & put appropriate measures in place; Mandatory Information Governance and IT Security training for all staff Data Protection is included in contract tracing service training (see appendix J). All staff have access to the PHA Information Governance policies and procedures through 'Connect' (PHA intranet site); All staff bound by HSCNI employment contracts Staff bound by professional regulatory Codes of Conduct Appropriate disciplinary action will be taken in the event of proven breach	Reduced	Low

13	Risk of noncompliance with established BSO ITS Service Transition Approval Process (STAP). Potential, in error, to negatively impact the MS Dynamics environment and therefore the contact tracing information system not be available (impacting on one tracers or entire contact tracing service user group)	Completion of documentation and approval by BSO ITS assistant director in line with existing governance applied to all HSC IT systems. Approved STAP documents are available to all BSO ITS staff for reference and are managed through established staff management mechanisms.	Reduced	Low
14	Risk of access to personal data by 3rd party processers. Potential impact of a data breach, with potential impact of distress or reputational damage to individuals. In addition the risk of reputational damage to the PHA.	No live system access rights are allocated to 3rd parties. All 3rd party access is in accordance with agreed contacts and contract management processes.	Reduced	Low
15	Risk of complaints/legal action from someone contacted by the service who feels that their Human Rights have been violated in that it has identified them as being in a certain place, with a certain person/persons.	Information provided to the tracers on the confirmed case, is not provided to the contacts. Close contacts are only informed of the date of the contact. CTIS separates confirmed cases and close contacts so confirmed case details are not visible within close contact screens. Privacy notice does remind people that confirmed case may be identifiable in some circumstances.	Reduced	Low
16	Risk that robust data sharing arrangements with not be in place for international transfers resulting in an inability to share data in respect of contacts with other countries outside of the UK especially after EU Exit.	Ongoing work with ROI to update and refine data sharing MOU particularly in light of a “no deal EU Exit”. With reference to port health an MOU for the	Maintain	Medium

	Potential impact of close contact not being contacted and associated risk of disease spread (no self-isolation).	sharing of data from the Home office national database for passenger locator forms has been agreed and signed by PHA and the Home Office. Working with PHE on wider national and international data sharing arrangements.		
17	Risk that personal data is used inappropriately for analytical purposes. Inappropriate sharing of personal data which could result in potential impact of distress or reputational damage to individuals. In addition, the risk of reputational damage to the PHA.	Current development of an Analytics Platform with involvement from all key stakeholders (including health protection, DHCNI). All staff involved are HSCNI employees and therefore must comply with mandatory Information Governance training. Access to the platform will be controlled via user management and allocation of appropriate rights and levels (eg read/write at various levels based on authorised need)	Maintain	Medium
18	Risk of fraudsters sending similar looking messages with malicious intent. Potential impact of distress or reputational damage to individuals, in addition the risk of reputational damage to the PHA.	Advice was sought from the National Cyber Security Centre (NCSC) to ensure that the SMS is as safe as possible. Sender ID based on guidance from the National Cyber Security Centre (NCSC) and SMS message content was also reviewed. Both have been classed as technically suitable by NCSC due to: The creation of some distance between SenderID and others nearby and the creation of a simple, recognisable link that is harder to mimic.	Reduced	Low
19	Risk of the DST being 'hacked', with the theft of personal identifiable data (data breach), with the risk of distress or reputational damage to individuals. Or the system being	Microsoft complies with both international and industry-specific compliance standards and participates in rigorous third-party audits that verify security controls. As required by the GDPR,	Reduced	**Medium**

	compromised or inaccessible as a result of a cyber security incident therefore contact tracing center being unable to operate with no positive cases or contacts being provided guidance on self-isolation etc. In addition the risk of reputational damage to the PHA.	Microsoft implements and maintains appropriate technical and organizational security measures, including measures that meet the requirements of ISO 27001 and ISO 27018, to protect personal data it processes as a data processor or sub processor on its customers' behalf. Microsoft follows the EU Standard Contractual Clauses (data resides in a secure cloud within the UK). All data is stored in the citizen's browser cache while being completed and no data is transmitted until the final page is reached and the submission button is clicked. Data is transmitted as a JSON data payload with TLS encryption to Microsoft Azure. Here it is placed in a submission queue from which is it submitted to Dynamics via the API. All data is encrypted in transit and at rest. Internal Penetration testing has been carried out by the 3rd party developing the solution. This process identified a small number of issues which have been addressed. External testing by a 3rd party, MDSec, has completed. Report produced (Commercial in Confidence) concluded that the web application was robust.		
20	Risk of fraudsters setting up a similar webapp as Digital Self Trace with malicious intent. Potential impact of distress or reputational damage to individuals, in addition the risk of reputational damage to the PHA.	Advice was sought from the National Cyber Security Centre (NCSC) to ensure that the SMS is as safe as possible. There is a large amount of material available via	Reduced	**Medium**

		website, apps etc to ensure the public are fully aware of what information will be required and why.		
21	SMS messaging failure could be missed by the system, meaning that positive COVID-19 citizens would not have a test code for use in DST.	See section 5.1.3	Reduced	**Medium**

9 Approval

Measures to mitigate risks have been approved and residual risks have been approved. Advice has been sought from the Data Protection Officer and reflected in the DPIA.

SIGN OFF	
Senior Responsible Owner/Information Asset Owner	
Name: Dr Gerry Waldron	**Date:**
Designation: Assistant Director Health Protection	
Project Manager	
Name: Jennifer Lamont	**Date:**
Designation:	
Director	
Name: Prof Hugo Van Woerden	**Date:**
Designation: Director of Public Health and Personal Data Guardian	

Appendixes

Appendix A – Data Processors and Sub Processors

All of the data processors are appointed under Data Processors Agreements in compliance with Article 28 of the GDPR. All data processors and sub-processor arrangements are managed via GDPR compliant agreements and contracts. The following provides a list of data processors and sub processors involved in delivery of the system.

- **Health and Social Care Board (HSCB)** act as a data processor on behalf of PHA. HSCB hold the contract with Kainos.

- **Public Health Agency (PHA)** act as data controller, as it is responsible for running the Contact Tracing Service and Analytics Platform, identifying the personal data to be collected, which individuals it is collected about, and how it is used.

- **Kainos** were chosen to develop the CTIS and analytic platform and are responsible for the configuration of the Dynamics system and are regarded as a sub-processor contracted by the HSCB, on behalf of PHA. Kainos will provide support on an ongoing basis to the CTIS configuration and analytic platform for the duration of its operation, as part of their contract. Their services are delivered via HSCB GDPR compliant contracts.

- **Business Services Organisation** statutory organisation providing services as a data processor for HSCB and PHA. They host the Central Test registry which provides information to the Contact Tracing System. They host the Dynamics platform (in line with their contract with Microsoft). BSO are responsible for monitoring and managing all Microsoft contracts as commissioned and monitored by HSCB. They are responsible for all three environments user access and provision of new user hardware (PC and phones). BSO ITS are responsible for the supply and maintenance of user hardware. PHA has an overarching SLA with the BSO for services including ITS. Their services are managed via appropriate agreements with PHA and HSCB.

- **Belfast Health and Social Care Trust (BHSCT)**

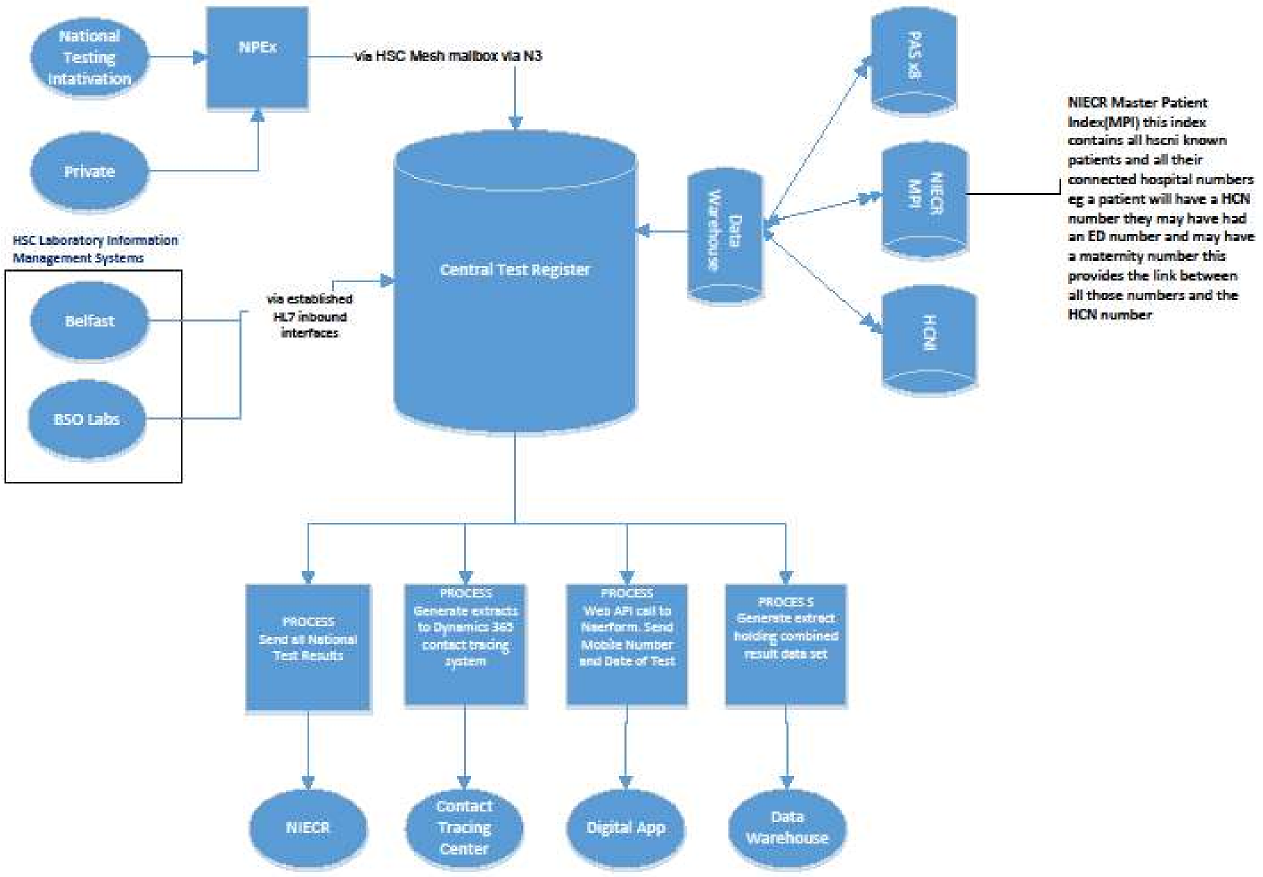
  BHSCT statutory organisation providing services as a sub processor for HSCB and PHA, through the BSO. BHSCT host the Digital Self Trace web application and analytics platform in line with their contract with Microsoft. PHA has an overarching SLA with the BSO for services including ITS. BSO have SLA's with all Trusts including BHSCT. Their services are managed via appropriate agreements with PHA and HSCB.

- **Microsoft** are responsible for, within the Microsoft Azure environment including the Dynamic 365 environment, software upgrades, security patching and updates for the Contact Tracing Information System; these are published via MS Office 365 portal that BSO ITS have access to. Microsoft will implement and maintain appropriate technical and organizational measures to protect Customer Data and Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Those measures shall be set forth in a Microsoft Security Policy attached. Microsoft make that policy available to customers, along with descriptions of the security controls in place for the Online Service and other information reasonably requested by customers regarding Microsoft security practices and policies. In addition, those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018. See appendix D for MOU, this will ultimately be included in existing contract between Microsoft and BSO (on behalf of HSCB). They are a sub-processor contracted by BSO (to provide this service).

Contracts and MoUs are in place to govern relationships with the above data processors and sub-processors which set out the obligations of each party and the data controller's obligations and rights with regard to the data that is being processed. All contracts adhere to established BSO Procurement and Logistics Services (PaLs) processes with legal input provided by BSO Department of Legal Services (DLS).

All data processing takes place within the EEA area, and as such is subject to legislation in the form of the General Data Protection Regulation (GDPR).

Appendix B – Central Test Registry


National Testing Intativation
NPEx
via HSC Mesh mailbox via N3
Private
HSC Laboratory Information Management Systems
Belfast
BSO Labs
via established HL7 inbound interfaces
Central Test Register
Data Warehouse
PAS x8
NIECR MPI
HCNI
PROCESS Send all National Test Results
PROCESS Generate extracts to Dynamics 365 contact tracing system
PROCESS Web API call to Naerform. Send Mobile Number and Date of Test
PROCES S Generate extract holding combined result data set
NIECR
Contact Tracing Center
Digital App
Data Warehouse

NIECR Master Patient Index(MPI) this index contains all hscni known patients and all their connected hospital numbers eg a patient will have a HCN number they may have had an ED number and may have a maternity number this provides the link between all those numbers and the HCN number

Appendix C Microsoft Security Policy

Adobe Acrobat
Document

Appendix D Microsoft MOU

Adobe Acrobat
Document

Appendix E HSC Code of Conduct

Adobe Acrobat
Document

Appendix F Contact Tracing Data Flows

Adobe Acrobat
Document

Appendix G Big Motive Research

Adobe Acrobat
Document

Appendix H HSC Regional Risk Matrix

Adobe Acrobat
Document

Appendix I Central Test Registry Processes

BSO assurances on the Central Registry Process:

Data Receipt

Data integrity is reliant on source Lab systems at this point. We have no mechanism to dispute the data integrity (specifically around patient identification). Whilst the quality of some of the data fields can be erratic, leading to processing errors, this is usually at a format level, rather than incorrect data itself.

Data Processing

HCN Validation and matching – we can present the list of queries that we run for this process. These are established by HCN Data Quality Team and have been used within the HCN for 10+ years, so our confidence in these is very high.

Anything that cannot be matched automatically is processed manually by the HCN team, which again is a standard business process that they undertake as part of their service, so confidence again is very high in this.

Matching Contact Numbers and Next of Kin – any matching is only undertaken on those records which have an HCN number. We are confident in this matching process. There is a caveat though, that the numbers and details returned from PAS systems are not verified by us, this is the understood responsibility of the CTC team at point of contact.

Data Transfer to CTC

Identification of Positive results was tested against the original manual process, to ensure counts and results were correct.

We maintain every file and record that we send to CTC, so that in case of a query we have an audit table to investigate and if necessary, resend the file.

Appendix J Contact Tracing Service Training Agenda

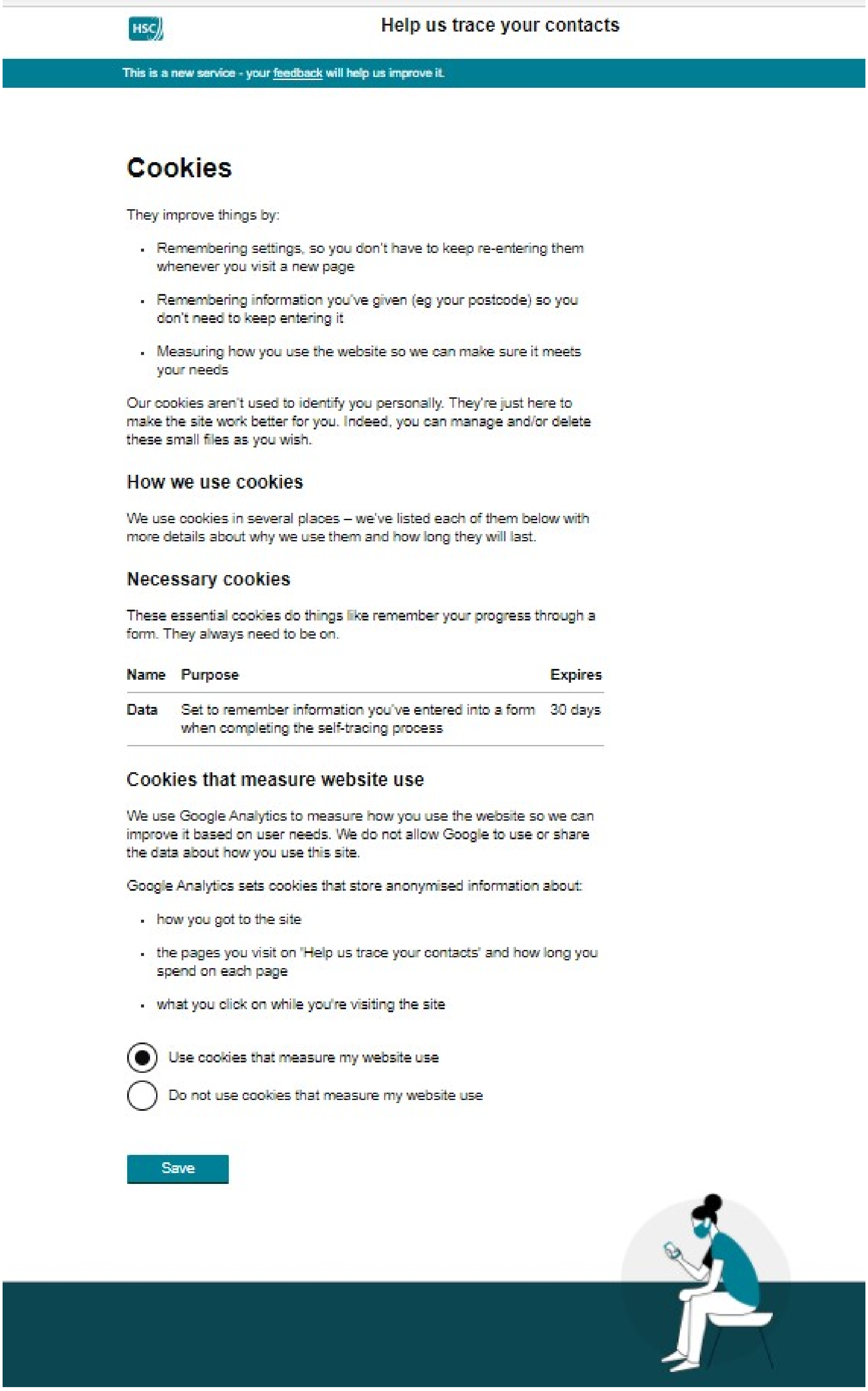
Adobe Acrobat Document

Appendix K for data flows of Digital Self Trace

Adobe Acrobat Document

Appendix L Cookie Policy for Digital Self Trace

This policy is accessible on the front screen of DST.



Help us trace your contacts

This is a new service - your feedback will help us improve it.

Cookies

They improve things by:

- Remembering settings, so you don't have to keep re-entering them whenever you visit a new page
- Remembering information you've given (eg your postcode) so you don't need to keep entering it
- Measuring how you use the website so we can make sure it meets your needs

Our cookies aren't used to identify you personally. They're just here to make the site work better for you. Indeed, you can manage and/or delete these small files as you wish.

How we use cookies

We use cookies in several places – we've listed each of them below with more details about why we use them and how long they will last.

Necessary cookies

These essential cookies do things like remember your progress through a form. They always need to be on.

Name	Purpose	Expires
Data	Set to remember information you've entered into a form when completing the self-tracing process	30 days

Cookies that measure website use

We use Google Analytics to measure how you use the website so we can improve it based on user needs. We do not allow Google to use or share the data about how you use this site.

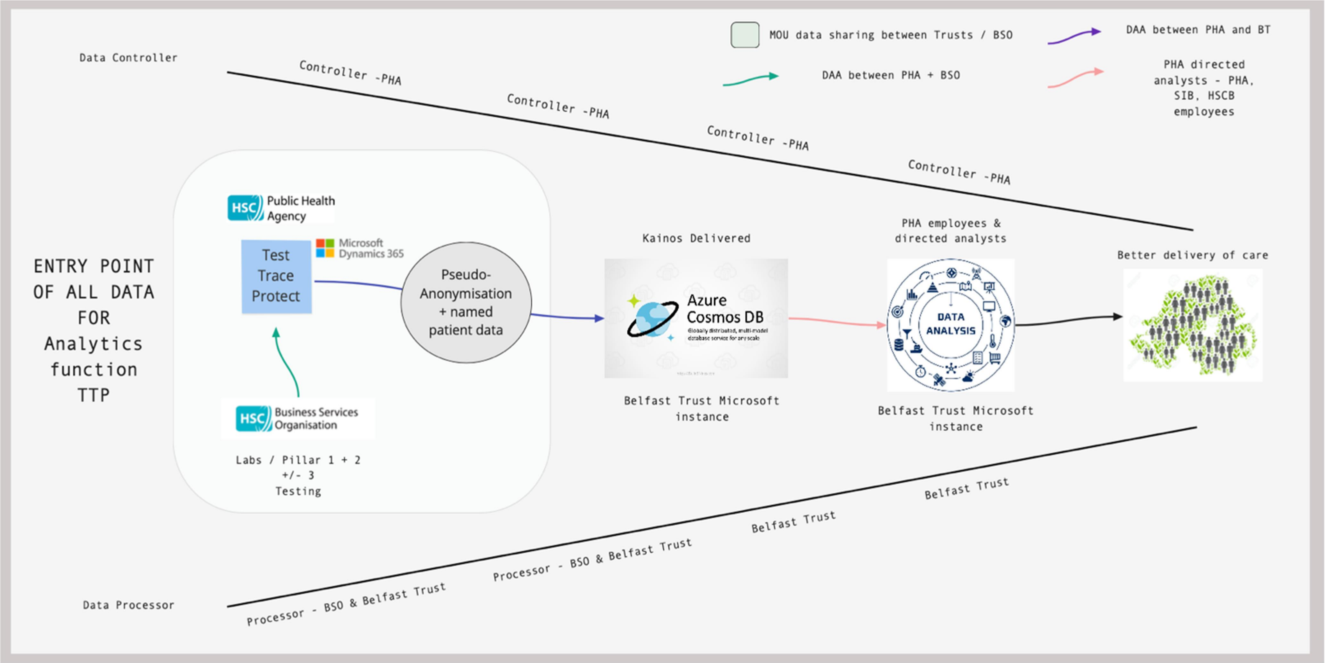
Google Analytics sets cookies that store anonymised information about:

- how you got to the site
- the pages you visit on 'Help us trace your contacts' and how long you spend on each page
- what you click on while you're visiting the site

● Use cookies that measure my website use

○ Do not use cookies that measure my website use

Appendix M Analytic Flow



MOU data sharing between Trusts / BSO
DAA between PHA and BT
DAA between PHA + BSO
PHA directed analysts - PHA, SIB, HSCB employees
Data Controller
Controller -PHA
Controller -PHA
Controller -PHA
Controller -PHA
ENTRY POINT OF ALL DATA FOR Analytics function TTP
HSC Public Health Agency
Test Trace Protect
Microsoft Dynamics 365
Pseudo-Anonymisation + named patient data
HSC Business Services Organisation
Labs / Pillar 1 + 2 +/- 3 Testing
Kainos Delivered
Azure Cosmos DB
Belfast Trust Microsoft instance
PHA employees & directed analysts
DATA ANALYSIS
Belfast Trust Microsoft instance
Better delivery of care
Data Processor
Processor - BSO & Belfast Trust
Processor - BSO & Belfast Trust
Belfast Trust
Belfast Trust