NHS Test and Trace

Data protection audit report

December 2021

Information Commissioner's Office

Executive summary

Background

At the start of the COVID-19 outbreak, Public Health England (PHE) carried out test and trace activities for the initial relatively low numbers of infections. As the infection numbers increased, the NHS Test and Trace programme (T&T) was introduced in May 2020. The primary objective of the programme was to "help break chains of COVID-19 transmission and enable people to return towards a more normal way of life" and this has involved the processing of data on an unprecedented scale in order to safeguard public health.

The Department of Health and Social Care (DHSC) has overarching responsibility for T&T and the Secretary of State for Health and Social Care has ministerial accountability. In October 2021 T&T was incorporated into the UK Health Security Agency (UKHSA).

The Information Commissioner's Office (ICO) engaged with the T&T in line with its regulatory response to the COVID-19 pandemic and its aim to ensure that information rights legislation does not pose an unnecessary barrier to organisations' response to the public health emergency, while encouraging the responsible use of information.

The ICO acknowledges that the T&T Programme was established at pace as a direct response to a major public health emergency and, as such, has been operating under acutely challenging circumstances and this fact has been taken into account whilst conducting the audit and producing this report.

Audit methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18) and other information rights legislation. Section 146 of the DPA18 provides the ICO with the power to conduct compulsory audits through the issuing of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

The DHSC agreed to a consensual audit by the ICO of the processing of personal data for the purposes of administering the T&T Programme. The primary purpose of the audit was to provide the ICO, DHSC and T&T with an independent opinion of the extent to which they (within the agreed scope this audit) were complying with data protection legislation and highlight any areas of risk to their compliance.

The scope areas covered by this audit were determined following a risk-based analysis of T&T's processing of personal data. The scope accounted for data protection issues and risks which were specific to the T&T Programme; identified from ICO intelligence or DHSC's own concerns, and any data protection issues or risks which affected their specific sector. The ICO further tailored the controls covered in each scope area to take into account the organisational structure of T&T and the nature and extent of their processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to the T&T Programme.

As a consequence of the risk based analysis it was decided to focus on the T&T Programme as a whole. For clarity, the functionality of the NHS COVID-19 App. was not included in the scope of this audit.

It was agreed that the audit would focus on the following area(s):

Scope area	Description
Governance & accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the UK GDPR and data protection legislation are in place and in operation throughout the programme.
Processor & third party supplier relationship management	Organisations should ensure there are effective relationship management controls in place with all processors and third party suppliers. Written contracts between controllers and processors are a requirement under the UK GDPR. These contracts must now include specific minimum terms. These terms are designed to ensure that processing carried out by a processor meets all the UK GDPR requirements, not just those related to keeping personal data secure.

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are normally a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

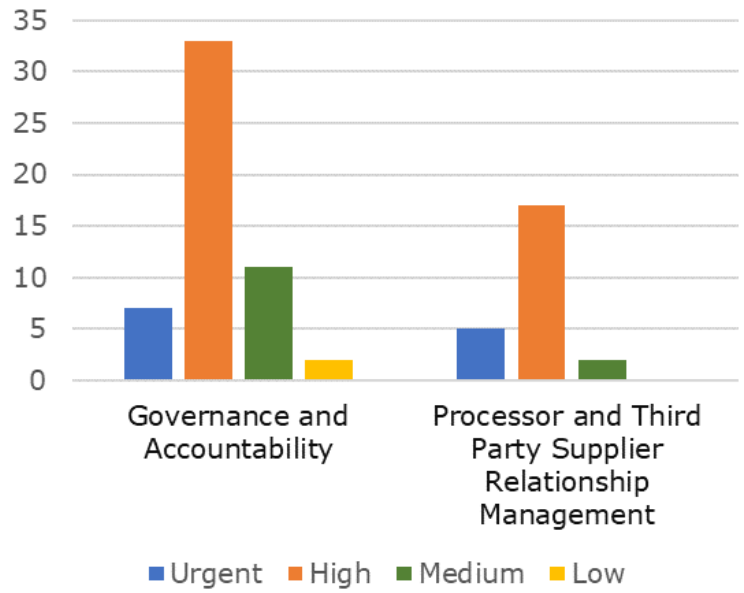
However, due to the outbreak of COVID-19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore, T&T agreed to continue with the audit on a remote basis. A desk-based review of selected policies and procedures, and remote telephone interviews were conducted between January 2021 and May 2021. The final audit report was provided to DHSC in July 2021. The ICO would like to thank the DHSC and T&T for their flexibility and commitment to the audit despite difficult and challenging circumstances.

Where weaknesses were identified, recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist T&T in implementing the recommendations, each has been assigned a priority rating based upon the risks that they were intended to address. The ratings were assigned based upon the ICO's assessment of the risks involved. T&T's priorities and risk appetite may vary and, therefore, they were advised to undertake their own assessments of the risks identified.

Summary of audit findings

As expected for an immature programme, the audit revealed a number of key requirements that were not yet in place. Steps were being taken to remedy some of these but processes had not yet been formally embedded. A total of 77 recommendations were made and progress against these will be assessed during the ICO audit follow up process, which will take place through the UK Health Security Agency (UKHSA) which took on operational responsibility for the T&T programme in October 2021.

Priority of recommendations by scope



The bar chart shows a breakdown by scope area of the priorities assigned to our recommendations made.

The governance and accountability scope had 7 urgent, 33 high, 11 medium and 2 low priority recommendations.

The processor and third party supplier relationship management scope had 5 urgent, 17 high, 2 medium and 0 low priority recommendations.

Main areas of progress to date

At the time of the audit, steps had already been taken to improve the privacy information made publicly available. The privacy notices seen met the requirements of Article 13 and 14 of the UK GDPR and provided enough information to inform data subjects about the processing of their personal data and enable them to enforce their data protection rights.
ICO Auditors were provided with a number of privacy notices used to inform data subjects about the processing of personal data by the T&T programme. Some of these are provided by the programme itself and others by organisations such as the NHS, NHS Digital, Public Health England (PHE) and venues where personal data may be collected to support the programme. Privacy information was found to be in line with ICO guidance in that it was concise, transparent, intelligible, clear, in plain language, and communicated in a way that is effective for the target audience.

Operational responsibility for information security within the T&T programme lies with the CISO Office which is headed by the Chief Information Security Officer (CISO) and a Deputy CISO. In 2020 it was identified that the existing resources for the CISO were insufficient, and a security consultancy was engaged to provide resources to build and operate the CISO Office. Most of the identified posts have now been filled but the structure of the CISO Office is still changing as a response to the processing activities being carried out.

Ultimate responsibility for T&T's information risk management lies with the DHSC Senior Information Risk Owner (SIRO).

The vast increase in the amount of personal and special category data being processed by the programme resulted in a need for increased oversight of information risk management. The SIRO heads the newly formed DHSC Information Risk Management and Assurance Directorate which will provide an information risk management function across the DHSC, it's Arm's Length Bodies and Executive Agencies.

Summary of priority areas for improvement

The following is a summary of the key urgent and high priority recommendations that were made.

T&T needs to ensure that information governance management structures are formalised and kept under review as they are embedded and, particularly after the handover from DHSC to UKHSA. Appropriate steering groups need to be put in place to provide oversight and assurance.

An appropriate information risk management structure needs to be put in place and appropriate policies and processes need to be developed. Processes need to include regular reviews of risk assessments. Information risk management training needs provided to staff who will be working in this area.

T&T's Information Governance policy framework is provided by DHSC policies which were being updated to reflect the processing being undertaken within the T&T programme. Other than the Acceptable use of ICT policy, T&T had no documented information security guidance for staff to follow. The DHSC policies were to be supplemented by T&T's own guidance but the majority of this was still in draft format and had not yet been finalised. A lack of key guidance means that T&T is at risk of non-compliance with the Accountability Principle of Article 5 (2) of the UK GDPR as well as increasing the risk of non-compliance with other data protection principles in Article 5.

T&T needs to carry out a comprehensive data mapping exercise to ensure that data flows are identified and reflected in relevant information asset registers (IARs) and within the record of processing activities (RoPA). Processes needed to be put in place to ensure that the RoPA and IARs are regularly reviewed and kept up to date.

In addition, the RoPA needs to be updated to include details of processing activities which involve data processors and third parties.

Some basic information security training had recently been mandated and rolled out within the T&T programme but the information governance training programme for T&T was not yet fully developed. Work had begun on creating a customised training programme, but this was not yet in place. There was also no process to gain assurance that contractors involved in the processing of personal data outside of T&T systems were completing any data protection training.

Staff, including those working for data processors and third parties, need to be trained in the provision of privacy information and its importance needs to be highlighted. Processes need to be developed to gain assurance that this information is being provided to data subjects in practice.

Due to its relative infancy, T&T had no formal information governance audit programme in place to ensure that information management and data protection compliance procedures were sufficient, effective, and met UK GDPR requirements. There was also no monitoring of compliance with data protection policies and procedures within the T&T programme. There was therefore no assurance that staff and third parties were following agreed processes which increases the risk of non-compliance with the UK GDPR Article 5 principles, including the possibility of a personal data breach.

A policy is required on sourcing, awarding and managing of contracts involving the processing of personal data by data processors and third parties. Data protection considerations need to be built into the contract approval and management processes including, where relevant, the completion of data protection impact assessments (DPIA). Where current arrangements have not been subject to some form of privacy risk assessment these should be undertaken retrospectively and action taken where required. Contract documents need to be reviewed to ensure that they include required technical and organisational safeguards and obligations in relation to breach reporting.

Monitoring of contracts with data processors and third party suppliers needs to be improved. Particularly in relation to ensuring that adequate training is provided to staff and ensuring that T&T is consulted prior to any subcontracting taking place. Periodic audits should be conducted with third parties to ensure that they are meeting their contractual obligations, including data protection and information security obligations and the results of these audits should feed into the information risk management processes.

Although processes were in place to ensure that any new processing activity undertaken by T&T is supported by written contracts, ICO Auditors were unable to gain assurance that this was also the case for all of the processing activity inherited by the T&T programme and the UKHSA.

Data protection by design policies need to be finalised and communicated to staff to ensure that a suitable privacy culture is embedded throughout the programme and that data protection requirements are considered at the outset of projects and process development activities.

Substantial progress had been made with DPIA and privacy impact assessment processes, but these had not yet been fully incorporated into the procurement and due diligence processes conducted before new contracts are entered into, including those with data processors.

The requirement for data processors to report all personal data breaches immediately, or as soon as identified, was not consistently documented in all data processing contracts, and there was insufficient detail on how those reports should be made. In addition, there were no processes in place to ensure that contractors had adequate data breach reporting processes or knowledge of those requirements before contracts were entered into. There were also no processes to provide assurance that third parties were complying with breach reporting requirements.

Response to the audit findings

UKHSA provided a detailed action plan outlining the response to each of the recommendations made. Of the 77 recommendations 71 have been fully accepted, 6 have been partially accepted and 0 have been rejected. NHS T&T have set out the actions that are intended to be taken to address each recommendation and the timescales within which they are intended to be completed.

UKHSA has also advised that the response to the ICO audit will form part of a wider project to develop its Information Management & Privacy (IM&P) Programme.

Having reviewed NHS T&T's response to our audit recommendations, alongside UKHSA's plans for its IM&P Programme, the ICO is satisfied that the proposed actions should allow the weaknesses identified by the audit to be addressed within a realistic and reasonable timescale, provided that sufficient resources continue to be made available for this work.

The ICO looks forward to reviewing the progress that has been made in addressing the audit recommendations when we come to undertake our follow-up audit.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance, and internal control arrangements in place rest with the management of NHS Test and Trace.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting, or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of NHS Test and Trace. The scope areas and controls covered by the audit have been tailored to NHS Test and Trace and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.