TIAN

Cyber Security Survey - The impact of Covid-19 on the NHS

Executive Summary

We received 43 anonymised survey responses from a range of senior IT professionals providing their views on how Covid-19 had impacted cyber-security within their organisation. This paper describes how the pandemic has changed the IT landscape within the NHS, as told by those behind the scenes (but very much at the forefront) of the NHS response.

The survey paints a picture of a monumental shift in not only the way we work internally but also how services are offered. These changes have brought many additional benefits to organisations:

- Increasing patient choice by giving more options how to receive consultations.
- Reducing barriers to service.
- Saving time for patients as well as service providers.
- Improved efficiency with the use of new communication tools including video conferencing.

IT departments have been vital in facilitating the change, working at an incredible pace to keep organisations as productive as possible. There have been many challenges to overcome including:

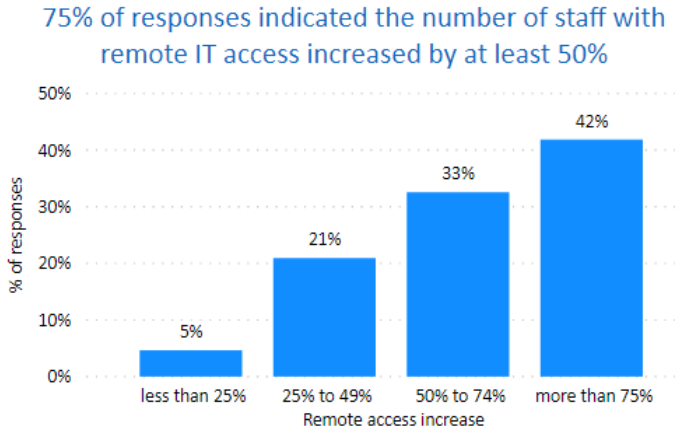
- Increasing IT workforce to respond effectively to the pandemic.
- Increasing remote worker access, as well as the infrastructure to support significant increases in active users.
- Mass procurement of devices to enable staff to work remotely.
- Rapid allocation of assets to many users across the organisation.

To achieve this in the time required, the majority of organisations relaxed certain procedures, often mitigated by risk assessments as well as plans for subsequent retrospective action.

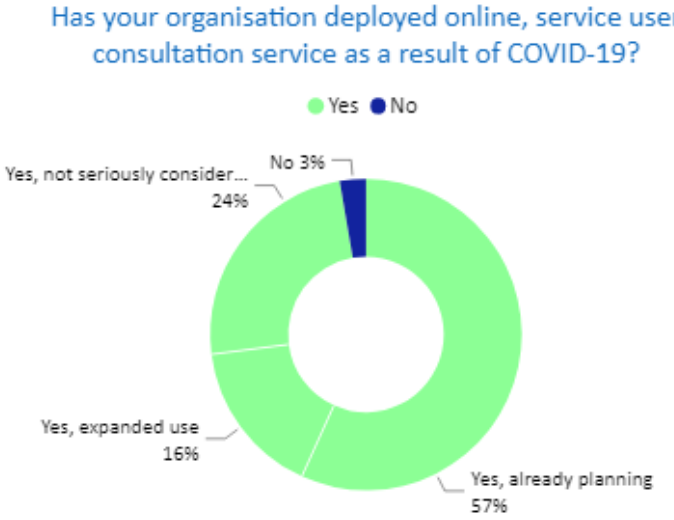
The detailed survey results and commentary are set out below and are followed by a number of questions you may wish to consider in seeking assurance.

Survey Results

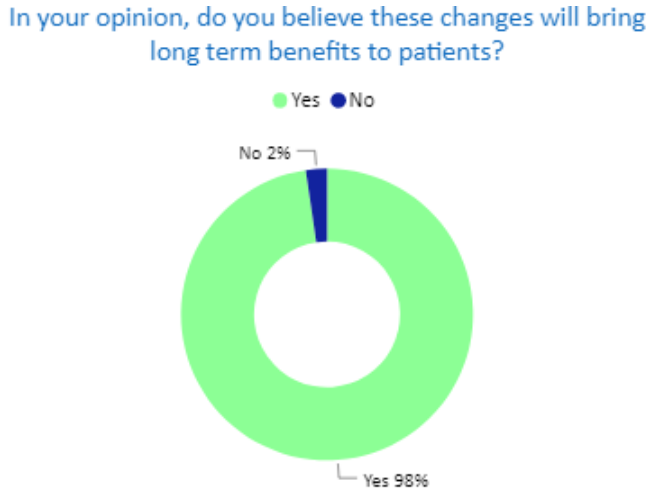
A period of transformation



COVID-19 has been a catalyst for change in the way NHS staff work. Where possible staff have worked at home, facilitated by the efforts of IT departments. 75% of survey responses indicated that they have increased the number of staff with remote IT access by at least 50%.



The pandemic not only changed the way staff communicate internally, but how organisations communicate with patients and service users. Organisations have deployed and expanded online consultation services to ensure consultations can continue where they would not be possible otherwise. A quarter of respondents indicated they implemented these services where they were not seriously planning to do so before.

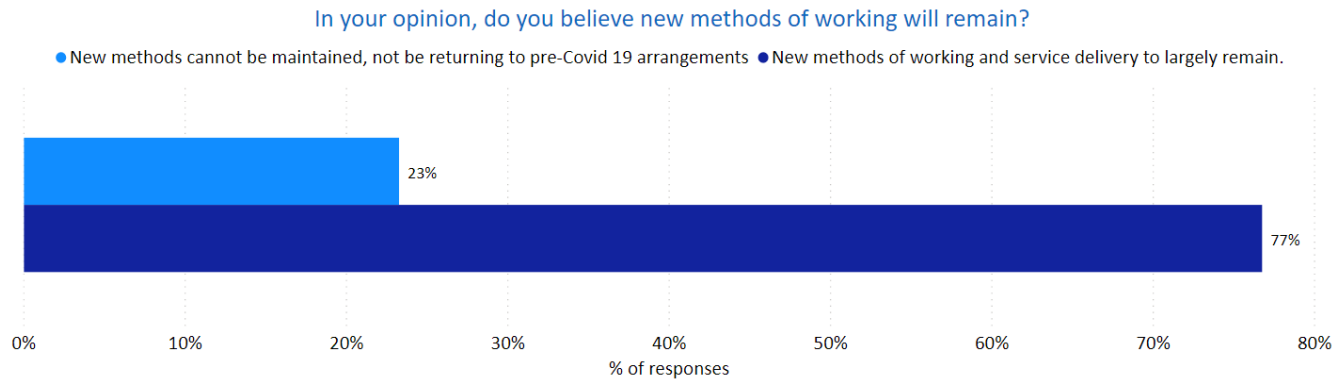


Senior IT professionals overwhelmingly believe changes forced by COVID-19 will bring long term benefits to patients.

Staff can work more flexibly and have more options for communication and collaboration.

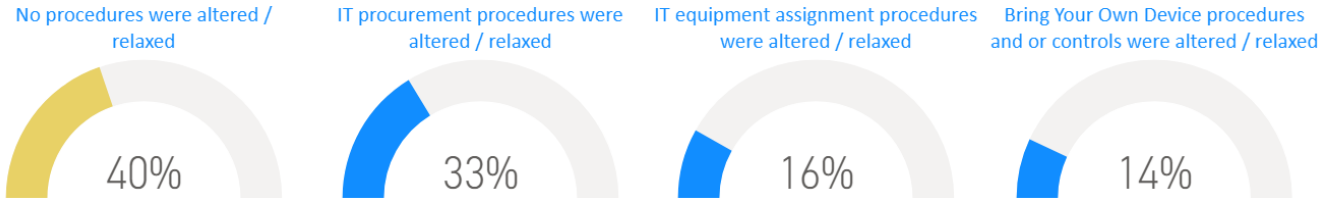
Online consultation services have the potential to improve patient choice in how they would like to interact with the service, as well as improving the efficiency of the service.

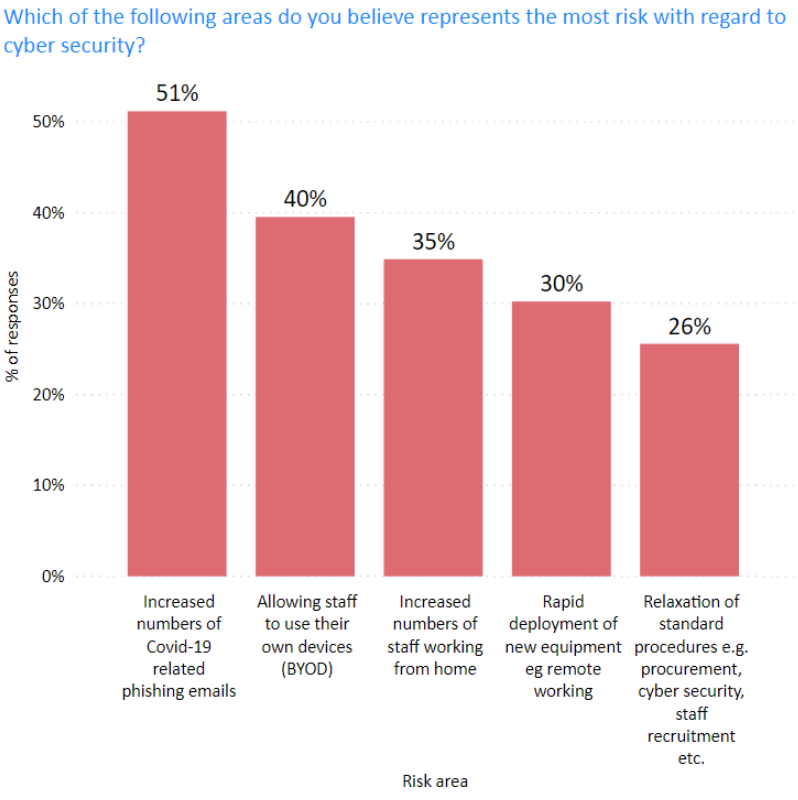
With this in mind it is unsurprising that 77% of responses considered that new methods of working and service delivery will largely remain. No respondents indicated they intended to fully revert back to pre COVID-19 ways of working, however one in five highlighted that new methods were not sustainable.



A rapid IT response

These changes presented a challenge for IT departments across all organisations surveyed. To enable staff to continue to work, IT expanded remote access capacity as well as procuring and distributing many devices, all at a rapid pace. To achieve this 60% of responses indicated at least one standard IT procedure had been relaxed/ altered. The most common procedures relaxed related to IT asset procurement and management, with a third of responses doing so in order to enable rapid procurement of devices.



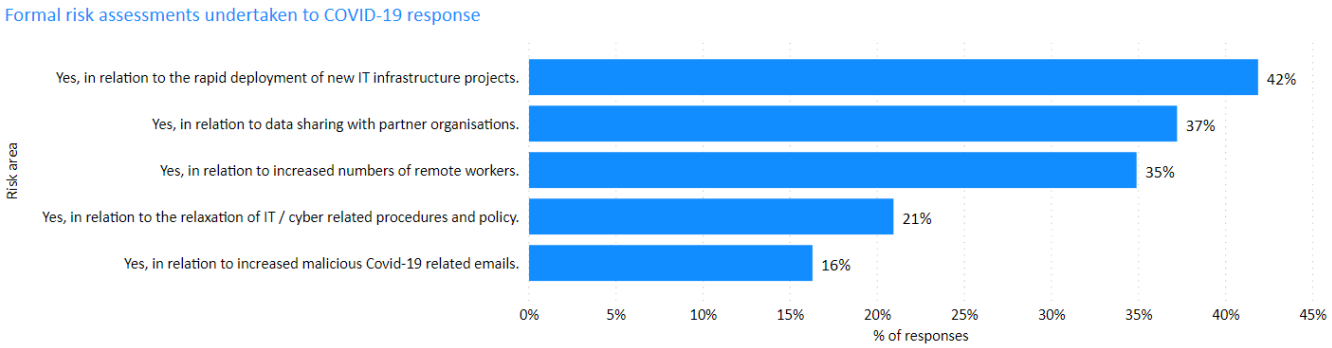


Several different cyber-security areas have been highlighted as high risk.

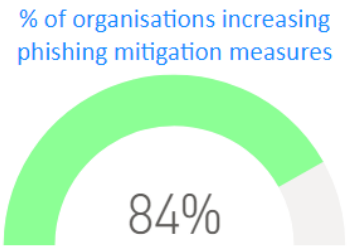
The most common risk is the increase in COVID-19 related phishing emails.

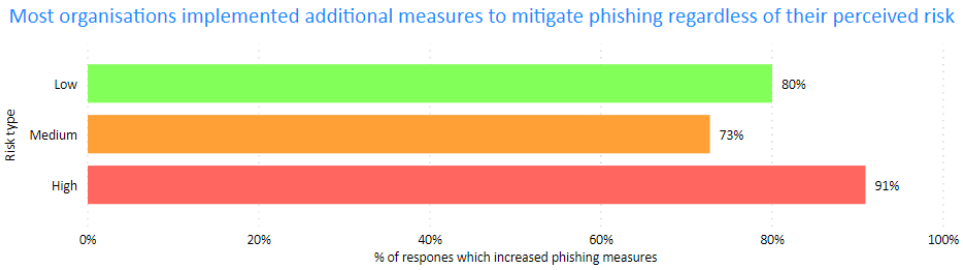
The relaxation of procurement procedures were considered least risky, also the most relaxed procedure. BYOD is the second highest risk area with few relaxing these procedures.

Formal risk assessments were not widespread in these areas. Rapid deployment received the most risk assessments assessed by 42%. COVID-19 related phishing emails were risk assessed the least despite being perceived as high risk.

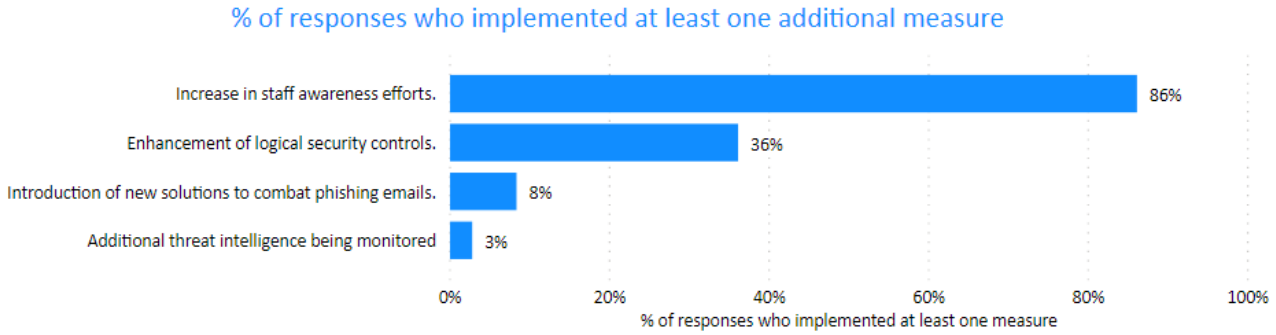


Most organisations have increased measures to tackle the increase in COVID-19 related phishing emails risk regardless of their risk rating. However one in ten organisations which rated the risk as high have not implemented any additional measures.



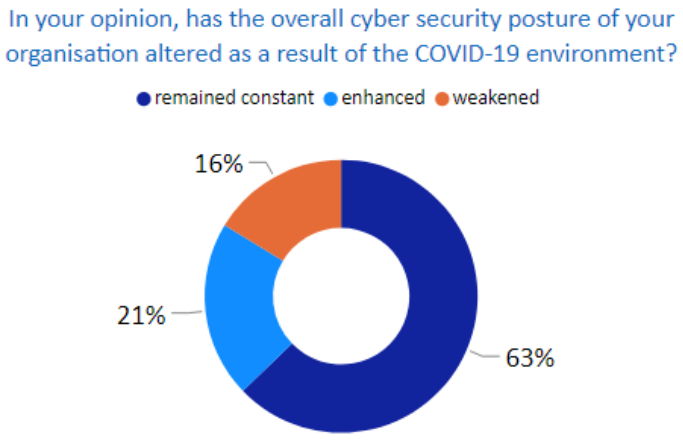


Organisations have focused their efforts on increasing staff awareness as the main way to mitigate the increased COVID-19 phishing emails, together with enhancement of logical security controls.



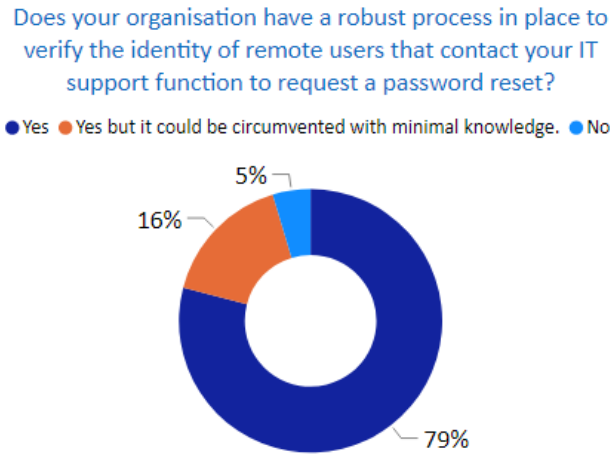
Despite having to progress large scale projects at pace, sometimes relaxing procedures in doing so, the overall cyber security posture of organisations is considered for the most part to have been either maintained or enhanced.

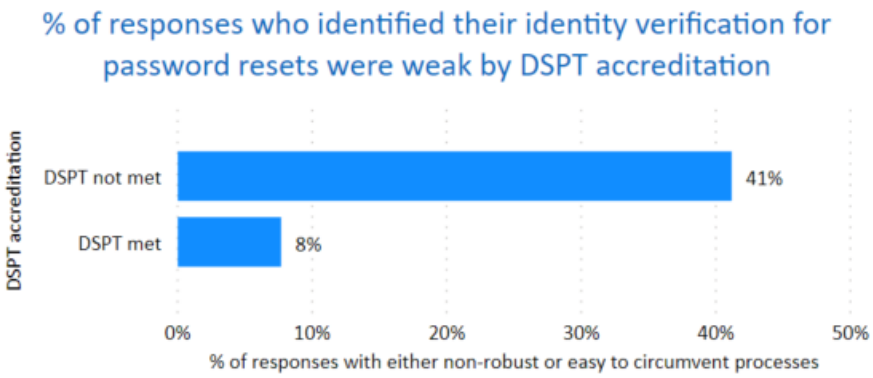
16% of responses did however indicate that they considered their security posture has weakened.



Areas to improve

One in five responses identified that their processes to verify the identity of remote users seeking to reset their password were either not robust or could be circumvented (with minimal knowledge). The exposure to this risk has increased with the increased number of remote users.

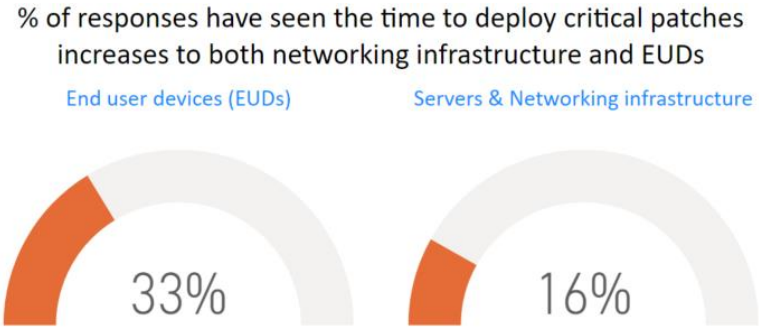




We noted a correlation with organisations' DSP Toolkit assessments.

A majority of those organisations reporting weaknesses in identity verification for password resets, also reported that they had not submitted a 'standards met' DSP Toolkit submission.

A number of organisations (albeit a minority) reported increases in the time to deploy critical patches, most notably to end user devices. This could be due to resourcing constraints and delays within IT, or a consequence of deploying and validating that patches have been applied, now that many more end users are working remotely.

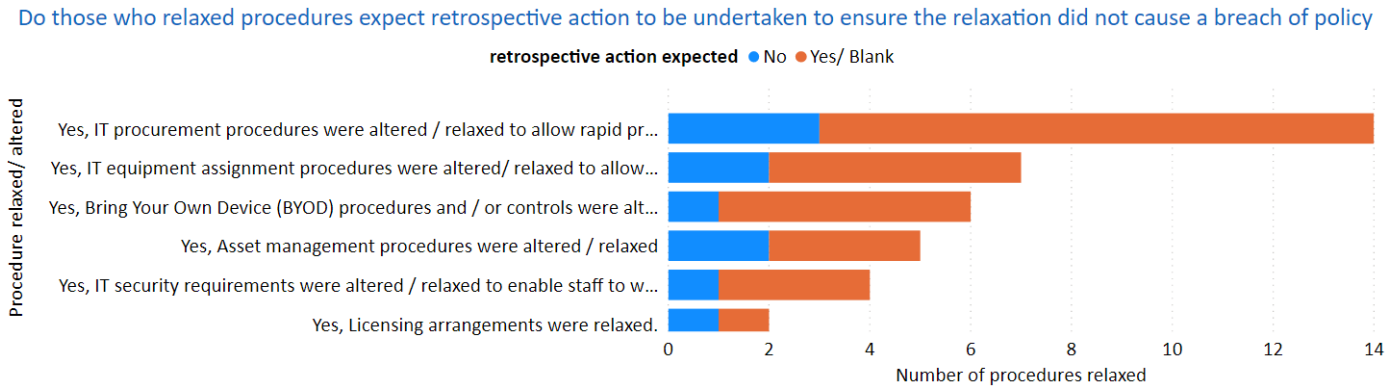


29% of responses who had relaxed at least one procedure have not planned for retrospective action to take place. i.e. to complete the governance checks that would ordinarily have taken place.

There might be limited benefit in the context of procurement where devices have already been purchased. It is still important however to ensure that asset configuration, deployment and management are all properly controlled, to ensure that weaknesses have not been introduced into the IT Estate.

Similarly it is important to evaluate whether relaxing any IT security requirements might have led to breaches, or have increased the risk of future breaches. These could include technical vulnerabilities (from the way that equipment is configured and used), or

information governance exposures (from the way that staff are working). An example might be whether patient information could be compromised when a clinician carries out a video consultation from their home. Is the home environment secure and soundproof, and if the clinician makes any handwritten notes, is there a robust process for filing or destroying those?



Gaining assurance over your current risk exposure

Responses to the survey presented a mixed picture of cyber security risks, highlighting the differing strengths and weaknesses between organisations as well as their diverging risk profiles. We have created some questions to help you gain assurance over your current risk exposure and if this is aligned to your organisations posture towards cyber security.

- If your organisation was required to rapidly procure and deploy assets, if this hasn't been accurately reflected in the asset register there is a risk that assets won't be properly utilised or could go missing or be stolen. Are you assured your asset register is up to date?
- Most organisations rated the risk of an increase in COVID-19 phishing emails as medium to high. The most frequent measure used by respondents was to increase staff awareness. Are you assured your organisation has taken sufficient action to mitigate the risk?
- Are you aware if your IT department relaxed standard procedures during COVID-19? If processes were relaxed, are you assured that these will not result in a breach, possibly with the use of risk assessments or retrospective action taken?
- 21% of responses indicated their processes for verifying identity to enable password resets were either not robust or easy to circumvent. Do you have assurance that your organisation's verification processes are robust?
- Achieving DSP Toolkit compliance improves IT processes as shown in the above detail where those organisations with better verification processes were those with compliant toolkits. Is your organisation making sufficient progress towards the DSP Toolkit compliance?
- Have you gained assurance that the increase in remote working has not caused delays in applying critical patches to end user devices?
- Almost a quarter of responders indicated current ways of working could not be maintained, but that they do not intend to go back to pre COVID-19 operations. Is your organisation aligned in how changes to the ways of working will continue post COVID-19? What are the restrictions to maintain the new way of working and do you understand the resources required to sustain new ways of working?
- If your organisation accelerated changes to or fully deployed an online, service user consultation service is it fit for purpose for both services uses and clinicians?

The Internal Audit Network (TIAN) is a professional network of NHS based internal audit providers, bringing together collective thinking to add greater value to our clients. TIAN is a membership network with a unique understanding and insight of the public sector, working with an NHS ethos aligned to public sector values. Our collective positioning across England and strong NHS client base continues to support valuable benchmarking and sharing of best practice.

On national and emerging issues, TIAN provides a vehicle to coordinate and channel professional opinion, working with key stakeholders to influence and engage on a national footprint. TIAN facilitates collaboration between providers and covers all aspects of internal audit including a wide range of associated specialist services such as anti-fraud, governance, assurance, security and risk management.

MIAA Improve the outcome

NHS The Leeds Teaching Hospitals NHS Trust

auditone

NHS West Midlands Ambulance Service University NHS Foundation Trust

cw audit

AUDIT YORKSHIRE The journey to excellence

ASW Assurance Sharing excellence in governance

360 ASSURANCE

NHS Guy's and St Thomas' NHS Foundation Trust

LONDON AUDIT

https://www.tian.org.uk/

For further information, please contact	**Andy Mellor** **Assistant Director** ☎ 07775 007 154 andy.mellor@nhs.net www.360assurance.co.uk 360 ASSURANCE