Guy's and St Thomas'
NHS Foundation Trust

REVIEW OF THE GUY'S AND ST THOMAS' IT CRITICAL INCIDENT
FINAL REPORT FROM THE DEPUTY CHIEF EXECUTIVE OFFICER
JANUARY 2023

Contents

1. FOREWORD

On behalf of the Trust Board, I welcome this report which draws together the findings of reviews into the major IT problems that affected our clinical systems last summer and had an unprecedented impact on the Trust's services.

Patient care was significantly disrupted, our staff were working without full access to the information they needed, and local GPs were unable to access test results.

On 28 July 2022 I issued a heartfelt apology to all those who had been affected by the incident, and I would like to take this opportunity to reiterate that apology. We know that during this period we did not meet the high standards we set ourselves on behalf of our patients, staff and partners.

Our immediate focus at the time was on restoring our IT systems as quickly as possible and reconciling all of the patient information that had been recorded on paper while these systems had been unavailable. We also committed to the commissioning of internal and external reviews to help us to understand exactly what happened and, importantly, to ensuring that we take every possible step to minimise the risk of similar problems arising in future. To have a lasting impact these reviews needed to be thorough, transparent, and completely honest about both the causes of, and the response to, the incident.

This report from the Trust's Deputy Chief Executive marks an important part of this process, and brings together the evidence that has been gathered to date from these reviews. I would like to thank all those who have contributed to these reviews and to this report.

Thankfully, while we recognise that patient experience suffered greatly during this period, evidence to date has identified no more than one case of moderate harm and no cases of serious harm to patients as a result of the incident. This is undoubtedly a testament to the expertise and dedication of our clinical and operational teams. Our staff worked tirelessly to keep our services running and to ensure that patient safety was not seriously compromised despite the significant challenges they faced. I would like to place on record my deepest gratitude to them. We will of course continue to monitor the situation closely and, should any further harm be identified, we will learn lessons and take action where required.

However, the report does identify areas where we could, and should, have done better, both in terms of our risk management systems which are designed to minimise the likelihood of adverse events, and also in how we responded to the situation once it occurred. The report includes a number of recommendations which have now been presented to and accepted in full by the Trust Board. They will be acted upon as quickly as possible.

The Trust self-referred the IT incident to the Information Commissioner's Office (ICO) for consideration under the UK General Data Protection Regulations due to the nature of the processing involved. I am pleased to say that, in December 2022, the ICO has closed its investigation with no regulatory action required.

Looking ahead, the introduction of our new electronic health record system in April 2023 will provide additional opportunities to update and consolidate our clinical systems and improve the resilience of our IT infrastructure.

Dr Ian Abbs
Chief Executive Officer
Guy's and St Thomas' NHS Foundation Trust

2. EXECUTIVE SUMMARY

2.1 Guy's and St Thomas' has good cause to be proud of its well-earned reputation among patients, staff and stakeholders. But when things go wrong, as they did so dramatically with the IT outage in summer 2022, the Trust must be ready to learn all lessons and act upon them decisively.

2.2 The Board committed at the outset of this review process to publishing the findings in the interests of transparency and learning, within the Trust and beyond. Patients, staff and partners should expect to be able to see a full explanation from the Trust of what happened and to be assured that there has been searching self-reflection.

2.3 Guy's and St Thomas' has 371 legacy IT systems that support patient records, patient administration, clinical services and infrastructure across Guy's Hospital, St Thomas' Hospital, Evelina London Children's Hospital and in the Trust's community services. These systems run on technical infrastructure housed in two data centres; the Guy's data centre situated in Borough Wing which was constructed in 2007 and the St Thomas' data centre located in a modular building which was constructed in 2012. The two data centres were designed to act as back-ups for each other in the event that one failed. The IT infrastructure was updated in 2015/16 as part of the Strategic Data Centre programme. Separate data centres support the IT systems at Royal Brompton and Harefield hospitals'.

2.4 On 19th July 2022, as had been forecast the preceding week, London experienced record-breaking high temperatures reaching 40°C. Over the course of the day, the two separate data centres at Guy's Hospital and St Thomas' Hospital suffered failures associated with the heatwave. This took down most of the clinical IT systems at Guy's, St Thomas' and Evelina London hospitals and in the related community services. The incident did not directly affect Royal Brompton and Harefield hospitals, except insofar as they provided mutual aid.

2.5 The Trust declared a critical site incident on 19th July and moved to implement a paper-based operating model ('Paper Hospital') to support clinical activity. On 21st July the Trust requested further NHSE and system support, raising the incident response from Level 1 (single organisation response) to Level 3 (NHSE London and SEL ICS system coordination). The technical recovery of IT systems took substantially longer than was anticipated at the outset, lasting several weeks before near complete restoration. The critical site incident was stood down on 21st September, having included management of the unrelated cyber-attack on an external supplier from 4th August onwards.

2.6 Clinical and operational teams went to extraordinary efforts to maintain clinical services and patient care. Nevertheless, the loss of IT systems caused widespread disruption to the running of clinical services and patient care within the Trust. There was also a significant impact on partners in primary care and on other hospitals in south east London, as system diverts were put in place for vascular and cardiac surgery, transplant patients, and some other specialist services.

2.7 A major and simultaneous failure of the data centres caused by an environmental event such as a heatwave was a risk that might have been predicted and was therefore potentially a preventable event. Whilst risk prediction, mitigation and reporting necessarily requires judgements to be made, and is not an exact science, it is self-evident that these processes did not adequately predict, mitigate or prevent this event. This represents a failure of the Trust's risk management processes to effectively mitigate the risk of data centre failure.

2.8 This review has found no single, egregious failure in the root cause analysis which has been carried out, but rather a combination of the following factors led to the catastrophic failure of the IT systems:

- sub-optimal cooling systems;
- ageing technological infrastructure;
- overly complex and distributed roles and responsibilities for managing elements of the data centre environment; and,

- partly linked to the previous point, insufficient cooling actions, both in terms of speed and scale, taken on the day of the incident to mitigate extreme ambient temperatures.

2.9 A thorough, comprehensive and independently chaired Harm Review is examining whether any harm came to patients as a direct result of the IT outage. To date the impacts, though widespread, have been predominantly short-term delays to care and considerable inconvenience to patients. These impacts should not be under-estimated as they fall far short of the experience that the Trust and its staff expect to provide to patients. There has been one moderate harm event identified to date, and 'duty of candour' communication has been completed as a result. That no other more serious harm events have been identified after rigorous review is a clear testament to the extraordinary skill, experience and professionalism of frontline staff. It cannot, at this stage, be ruled out that further harm events may be identified, and the Trust must remain vigilant to this possibility as the Harm Review is completed.

2.10 It is abundantly clear, from the listening events held as part of this review, that the incident took a heavy toll on staff, who reported fatigue, stress and an adverse impact on morale. In particular, this affected frontline clinical and operational staff, who worked tirelessly to provide safe patient care, and also the IT team who worked tirelessly, often around the clock, to recover critical IT systems under immense pressure. The Trust must be deeply self-reflective about the impact on staff, which comes after a long period of difficult working conditions during the COVID-19 pandemic, and must therefore ensure that psychological and well-being support is readily available to all who may need it.

2.11 Once the IT outage had occurred, the Trust responded rapidly through its well-established incident response protocols. The fact that these protocols have been so heavily used in recent years, including during the pandemic and other major incidents, was both a strength and a weakness. While they are well practised and understood, there is undoubtedly a sense of 'incident fatigue' amongst staff after all they have faced in recent years. The Trust initially under-estimated the probable duration of the IT incident, and this was reflected in the Trust's communications during the first few days, which was felt by many staff and stakeholders to under-play the severity of the situation. This was exacerbated by the loss of some of the most important communications channels, including the Trust intranet, which were affected by the incident. Once there was a greater understanding of the potential duration and impact of the incident, the Trust's communications were quickly adjusted to be more frequent and to reflect the severity of the situation.

2.12 Whilst the operational response to move to a 'Paper Hospital' was managed with speed and determination, there was widespread frustration with how long it took to recover core clinical IT systems: several weeks rather than hours or days. This was not a reflection on the effort or professionalism of the Trust's IT team, but demonstrated the limited number of individuals who had a detailed understanding of the Trust's legacy IT systems which were too numerous, complex and inter-linked to be recovered quickly.

2.13 The Trust must never again allow itself to be in a situation where the recovery of its core IT systems, whether as a result of infrastructure failure, cyber-attack or another cause, takes so long to complete. As a result, the Trust must put in place a comprehensive strategic plan, backed by appropriate investment, to ensure future computer processing and data storage requirements are robust, able to meet growing demand and also resilient to foreseeable risks. These plans should include periodic and thorough testing of systems recovery.

2.14 Implementation of a new electronic health record system, provided by Epic, in April 2023 will be a key part of the rationalisation and consolidation of legacy IT systems. A decision has already been taken to progress with this implementation as it will improve future resilience, albeit with a minimally adjusted timescale to recognise the disruption to the programme caused by the IT incident.

2.15 It was deeply unfortunate that an unrelated national cyber-attack on the systems provided by an external supplier, Advanced, occurred in early August and affected the CareNotes and Adastra medical

records systems used in the Trust. This was completely outside of the Trust's control and affected NHS organisations across the country. Nevertheless, for the Trust's staff, particularly those working in community services, the cyber-attack was a compounding factor that made it difficult to provide patients with safe and reliable care. These systems were eventually restored in early December, although the process of reconciling patient records is a major undertaking and was ongoing at the time of writing.

2.16 The Trust must prepare for the fact that climate change means extreme weather events are expected to become more frequent and challenging in future. It has therefore commissioned expert advice on how to ensure greater resilience for both its digital and physical infrastructure in light of these threats. Our response to these findings is expected to lead to some changes to the Trust's backlog maintenance and capital investment programmes.

2.17 This review has attempted to understand what occurred during the IT incident, and why, including the impact on patients and staff. It also sets out the actions that the Trust should take to rebuild trust, to care for those affected, and to ensure a similar event cannot happen again. We are grateful to all those who have participated in the review process and who have given their views with candour and thoughtfulness in the spirit of learning all the lessons from this deeply regrettable incident. The Trust Board should now receive, consider and agree to implement the recommendations in this report with humility and self-reflection.

3. BACKGROUND

3.1 On 19th July 2022, as had been forecast the preceding week, London experienced record-breaking high temperatures reaching 40°C. Over the course of the day, the two separate data centres at Guy's Hospital and at St Thomas' Hospital suffered failures associated with the heatwave. This took down most of the clinical IT systems at Guy's, St Thomas' and Evelina London hospitals and the related community services. It did not directly affect Royal Brompton and Harefield hospitals, except insofar as they provided mutual aid.

3.2 The IT outage impacted 371 clinical and non-clinical IT systems, including:

- electronic patient records – meaning clinicians were unable to access the medical records for patients they were treating;
- electronic prescribing systems – disrupting electronic prescriptions and dispensing;
- electronic ordering for investigations – requiring clinicians to order tests and investigations through more cumbersome paper processing, and
- e-Notation – preventing electronic inpatient and outpatient clinical note taking.

3.3 Clinical and operational teams went to extraordinary efforts to maintain clinical services and patient care. Nevertheless, the loss of IT systems caused massive and widespread disruption to the running of clinical services and patient care within the Trust. There was a significant impact on partners in primary care and on other hospitals in South East London, as system diverts were put in place for vascular and cardiac surgery, transplant patients, and some other specialist services.

3.4 During the outage of the primary patient information systems (weeks ending 24th and 31st July), the Trust's activity fell significantly. In some cases, services had to pause completely, where a paper work-around was not viable. Compared to the historic average levels for July, there were only:

- 64% of referrals received;
- 84% of outpatient appointments;
- 71% of elective surgical admissions; and,
- 68% of diagnostic tests.

3.5 The Trust incurred £1.4m out-of-plan spending on technology services to respond to the incident. This included a cloud-hosted environment to provide resilience for data backups, and a third-party specialist recovery service to image and extract data from the corrupted disks damaged during the data centre failure.

3.6 In addition to those readily quantifiable impacts, the critical incident had a profound and negative impact on the experience of care and of working at the Trust for many thousands of patients and staff. On 28th July, the Chief Executive issued a full and heartfelt apology on behalf of the Trust and its Executive Directors. The Chief Nurse also apologised to patients and staff, on behalf of the Trust, on Thursday 28th July, in an interview with BBC London.

3.7 The Trust managed the IT outage as a critical incident under Emergency Preparedness, Resilience and Response (EPRR) protocols. The incident was declared on 19th July and stood down on 21st September.

3.8 The management of, and recovery from, the critical incident was complicated by the unrelated national cyberattack on Adastra and CareNotes systems, which impacted the Trust, particularly its community services, and NHS organisations across the country.

4. REVIEW METHODOLOGY

4.1 The Chief Executive commissioned a number of internal investigations on behalf of the Board of Directors (the Board), which have been complemented by external work commissioned by South East London Integrated Care System (SEL ICS) and NHS England London region to ensure objectivity and accountability.

4.2 This review has been wide-ranging and engaged specialist knowledge and external validation where appropriate. The review has sought to answer six principal questions:

(i) How did the data centre failures happen?

(ii) How did the Trust's risk management systems and approach operate in this case?

(iii) Did any actual or potential harm come to patients by omission or commission of care?

(iv) Has the Trust fully understood the impacts on staff so that they can be supported appropriately?

(v) How effectively did the Trust manage the incident response?

(vi) What other actions should the Trust take to improve infrastructural resilience to potential extreme weather events in the future?

4.3 Given the different types of expertise required to answer these questions fully, and the need for both internal learning and external scrutiny, this review brings together nine separate strands of investigation. Six internally-led investigations have been complemented by three externally-led pieces of work (commissioned by South East London Integrated Care System and by NHSE London region).

4.4 A summary of the Terms of Reference for each strand of the review are set out in Annex A Main findings and recommendations are listed throughout the sections of the report and consolidated at the end of the main report for ease of reading.

4.5 The review process has been managed by the Deputy Chief Executive, supported by a GSTT coordination group including Internal Audit, the Freedom to Speak Up Guardian, General Counsel, Quality and Assurance, Essentia, Data, Technology & Informatics (DT&I), EPRR and Corporate Affairs.

4.6 This report will be presented to the Trust's Audit and Risk Committee and then reported publicly to the Board of Directors, as well as to external bodies where appropriate. In addition, the outcome from the Harm Review will be reported to the Quality and Performance Committee of the Board. In order to ensure openness and transparency, the Board has committed to publish the main findings of this review through a Board report.

4.7 The review has been conducted with the following guiding principles in mind:

- **Humility** – The Trust recognises this was a major failure of core operating systems, which seriously let down patients, staff and partners. The Review has sought out and listened with humility to the experiences and accounts of affected patients and staff.
- **Learning and accountability** – This review has been about understanding fully and learning all lessons from the events that took place. The Trust must be accountable for acting upon those lessons without fear or favour.
- **Transparency** – The Board committed at the outset to publishing the review findings in the interests of openness and learning, within the Trust and beyond. Patients, staff and partners should expect to be able to see a full explanation from the Trust of what happened and to be assured that there has been searching self-reflection.
- **Objectivity** – The review has strived to maintain objectivity, ensuring a separation of responsibilities between those who led the response to the incident and those who led the review into it. For the

review into patient harm, an independent chair has been appointed. NHS England London region and the South East London ICS are ensuring there is external scrutiny, accountability and objectivity. Relevant information will be provided additionally to the Information Commissioner's Office.

- **Timeliness** – Given the potential impacts on patients, staff and partners, the Trust Board recognised the need for the review to report in a timely fashion, so that lessons can be learned and acted upon expediently.
- **Thoroughness** – However, the Board is also committed to ensuring the review is thorough, considers all aspects of the incident and its impacts and that pace is balanced with rigour.

4.8 Strenuous efforts have been made to hear from staff and patients affected. The Trust has provided easily-accessible opportunities for patients, staff, system partners and other affected stakeholders to share their views and experiences. In addition to the Freedom to Speak Up advocate network, the Trust set up a dedicated email inbox (ICTincidentreview@gstt.nhs.uk) for staff to share any concerns, information or feedback. Trust-wide communications were issued, setting out the approach to learning lessons from the incident and providing details of how staff could get in touch. The review process was taken proactively to key staff forums and meetings, including staff-side engagements and Governor's meetings. The anonymised voices of some of those affected are included at various stages in this report.

4.9 The review has followed a root cause analysis approach to understanding the critical incident, with three primary goals:

(i) to discover the root causes of the IT incident;

(ii) to fully understand how to fix, compensate or learn from any underlying issues within those root causes, and

(iii) to apply what is learned from this analysis to systematically prevent future issues.

4.10 At the time of writing this report, the review work has been substantively completed, with sufficient thoroughness to draw main findings and recommendations. The main findings and recommendations, once agreed by the Trust Board, will be published in a timely manner, allowing the Trust to act promptly on the recommendations. Some elements of the investigations will continue beyond the publication of this report, and any further findings that emerge will be presented to the Trust Board. A follow up report will be published in due course if necessary. Specifically, the ongoing work consists of the following:

- the harm review will remain open. While the bulk of the work has been completed, the review will continue until all records have been reconciled and Structured Judgement Reviews (SJRs) have been completed into all deaths that occurred before the end of September 2022. This goes beyond the point that the majority of IT systems were restored to ensure that any deaths after a delayed period are captured in the SJRs, and
- the IT review commissioned by NHS England London region has been set up to build on and scrutinise the conclusions from the GSTT internal investigations. Therefore this external review was planned to run to a different timeline, following the initial GSTT reviews. NHS England have established a review panel that met for the first time on 14th November 2022.

5. TIMELINE OF EVENTS

The following timeline describes the relevant events prior to the critical incident, during the incident itself and the recovery phase. Incident definitions, including levels, are explained in Annex B.

The following is a brief summary of the main organisations or departments referred to in the timeline:

DT&I – GSTT's in-house Data, Technology & Informatics Directorate;

Essentia – GSTT's in-house estates and facilities management group;

ATOS – Private company responsible for managing the data centres;

NetApp – Manufacturer of the data centre storage network equipment; and

Secure IT – Third-party company responsible for servicing the data centre air conditioning.

2007 – Guy's data centre is built and the operational running is handed over to IT (now DT&I).

2012 – St Thomas' data centre is relocated to a specialised modular build under Gassiot House.

August 2018 – A report on the St Thomas' data centre by Secure IT identifies that the air conditioning condensers are not optimally situated for air flow. The report recommends the condensers are moved. Mitigating actions are taken but the condensers are not moved.

December 2020 - Atos, GSTT's strategic partner for future Epic infrastructure, take over day to day management of the existing datacentre IT Infrastructure from the original supplier & support partner ANS at the Trust's request.

March 2021 – A third-party inspection by Secure IT reports that the Air Handling Unit (AHU) at the Guy's data centre will approach the end of its life in 2021/22.

Feb 2022 – Secure IT revise their assessment of the AHU at Guy's, reporting that it will approach end of life in 2022/23. A Request for Funding for replacement is raised to the DT&I backlog maintenance fund.

June 2022 – The air conditioning units for the data centres at the St Thomas' and Guy's sites are cleaned and serviced. No new concerns are raised at this stage.

5th July 2022 – Media reports expectation of 40°C temperatures in the UK, due around 16th July.

15th July 2022 – The Met Office forecasts temperatures above 40°C for the first time in the UK. The first ever red warning for exceptional heat is issued. The previous highest recorded temperature is 38.7°C, in Cambridge, in 2019. At **11:00**, the Trust Heatwave Tactical meeting took place and agreed action responsibilities for the Hot Weather Plan. This includes a specific action on monitoring the temperature in the data centres, something DT&I do as business as usual, but calling out the specific need to do this particularly in the hot weather. At **14:52** the Telecoms Infrastructure Manager (within DT&I) sent a group email to the infrastructure team to monitor temperatures within the data centres, in light of the high temperatures, and flagging that there may be a need to hose down the condensers. This email only referenced the St Thomas' data centre, as it was the one where temperature control was considered a risk.

18th July 2022 – Temperatures in London peak at 37°C. The highest temperature recorded in the St Thomas' data centre is 26.5°C. Despite high ambient temperatures that day, no untoward temperature issues are recorded in either data centre. The St Thomas' data centre storage array is backed up, using the routine fall-back solution Commvault. At **08:00**, a serious site incident is declared at GSTT for the general effects of the hot weather. Command and control procedures are activated in line with the serious site incident protocols.

19th July 2022 – London hits record temperatures up to 40.3°C.

Guy's Data Centre

11:29: The first high temperature alert (26°C) at the Guy's Hospital data centre is recorded.

11:54: DT&I team at Guy's data centre request a Secure IT engineer to attend the Guy's site.

12:30 (approx.): The minimum reading across a number of sensors for humidity in the Guy's data centre drops below the recommended level of 20%. Senior management are notified of the rising temperatures.

12:50: Guy's Data Centre suffers an air conditioning failure as the high-pressure trip-switch is activated, causing the unit to shut down. Initially, a single unit shut down (12:18), but this was followed by a cluster of 17 trips over 40 minutes, with more throughout the rest of the day. This air conditioning failure led to a rapid rise in temperatures within the

13:34: DT&I staff and ATOS staff start a controlled shut down of parts of the infrastructure in an attempt to reduce temperatures.

13:55: The Secure IT engineer (requested 11:54) arrives at **the** Guy's data centre site.

14:10: The Secure IT engineer begins cooling the condensers at the Guy's data centre. The temperature in the data centre is now 45°C.

14:16: The temperature inside the Guy's data centre reaches 50.3°C. The normal operating temperature is around 20°C.

14:58: Essentia provides a mobile ventilation unit for the Guy's data centre.

St Thomas' Data Centre

12:05: The external sensor at the St Thomas' data centre, which recorded the temperature near the condensers, identifies rising temperatures (a specific number was not recorded). DT&I request support from Essentia to cool the data centre.

13:15: The St Thomas' data centre records a temperature of 25° and rising. The maximum operating temperature limit is 40°C. The target temp is 20°C.

13:28: Connection to the remote data centre environment monitoring solution for the St Thomas' Data Centre (hosted on the SAN) is lost.

13:30: Attempts to cool the St Thomas' data centre begin, by hosing cooling units with cold water, but are hampered by difficulty connecting the hose to a water supply.

14:01: Sensors detect humidity below the target operating level of 20%.

14:12: One of the two compressors trips within one of the four air handling units at the St Thomas' data centre.

14:16: The St Thomas' data centre hits 36.2°C, with humidity below 20%. Email alerts stop working due to Controller / Disk failures.

14:22: ATOS receives reports of numerous disk failures at the St Thomas' data centre.

18:04: Multiple disk failures, unrecoverable errors and system failures reported at the St Thomas' data centre up to 22:00.

Whole Trust

08:50: Temperatures of 31°C are recorded at London City Airport.

13:06: ATOS receives an automated notification that a shelf within the St Thomas' data centre is recording a temperature of 43°C. This shelf was not part of the Storage Area Network (SAN) that would later fail and continues to function. ATOS receives a report of a single rack shelf at the Guy's data centre reaching 43°C. The first email to GSTT from ATOS notifying them of this is at 13:33, after manual cooling efforts have begun.

13:20: The London ambient temperature peaks at 40°C[2].

14:00: Connectivity issues are reported with the Cancer System, GTi (intranet), ATOS Network, Snapcomms and Solarwinds.

14:15: Connection to call centre servers hosted on the SAN are lost. Telecoms team experience disruption and revert to contingency arrangements. No subsequent alert data are recorded after this point.

14:26: Clinical Alert issued internally at GSTT, describing intermittent disruption to multiple Trust IT systems.

14:30: Intermittent disruption to multiple IT systems Trust-wide is first reported. This includes Core Network Internet, Cancer Centre, Telephony, Symphony, MedChart, Self Check-in, Call forwarding and VPNs. The Incident Log records the decision to declare a Critical Site Incident.

15:00: A Critical Site Incident is communicated to staff with an email Clinical Alert and the incident is reported to NHS England. The Trust enacts business continuity arrangements and moves to paper for all clinical applications.

17:20: Data centres at St Thomas' and Guy's are both now reporting normal operating temperature ranges.

17:45: Clinical Alert issued, declaring a move to 'Paper Hospital'.

20th July 2022 – GSTT Wi-Fi network and Virtual Private Network are restored. "Message from the Chief Executive" issued to staff, discussing the disruption from the heatwave and, in particular, the IT outage. Regular updates from the Chief Executive follow from this point.

21st July 2022 – GSTT request further NHSE and system support, raising the incident response from Level 1 (single organisation response) to Level 3 (NHSE London and SEL ICS system coordination).

23rd July 2022 – Tactical command structure is expanded to include a number of formalised sub-groups.

24th July 2022 – Symphony (the Emergency Department IT System) functionality begins to be restored. Functionality is not restored smoothly and users report malfunction in the early recovery period.

26th July 2022 – PIMS (patient administration system) reconciliation begins.

26th July 2022 – First daily all staff update from the Chief Digital Information Officer outlining which systems have been switched back on and which are next in line for restoration. These will run until the end of August, supplemented by regular MS Teams briefings.

27th July 2022 – Outpatients restarts electronically.

28th July 2022 – Ordering for Pathology and Imaging requests returns to fully electronic ordering via Electronic Patient Record for all inpatient wards and the Emergency Department.

28th July 2022 – The Trust Chief Executive issues public apology to all patients, staff and local community.

29th July 2022 – e-Noting is restored for outpatients and all new admissions. Reconciliation starts for all inpatients, including those in community bedded units. MedChart (electronic prescribing system) is restored.

3rd August 2022 – New rotation of Foundation Year 1 trainee doctors joins the Trust. Foundation and core trainees will continue to rotate throughout August.

4th August 2022 – NHS supplier, Advanced, is hit by a national ransomware attack, impacting access to Adastra and CareNotes medical records. The attack is unrelated to the GSTT IT Incident, but compounds the operational challenges, especially for community services. DT&I operational staff carry out additional checks to confirm that the Cyber Attack on Advanced had not spread to the GSTT infrastructure. This separate incident would continue for months.

5th August 2022 – The Trust Chief Executive, Chief Medical Officer and Chief Nurse issue a joint statement to staff reassuring them that they have the full support and commitment to the decisions they have made and continue to make based on professional judgements in line with standards of clinical practice.

22nd August 2022 – Strategic and Tactical Command group meetings shift to a recovery focus and the Critical Site Incident is downgraded from a Level 3 system response to a Level 1 internal critical site incident response.

23rd August 2022 – The Trust Chief Executive, Chief Medical Officer and Chief Nurse issue a second letter to colleagues, thanking them for their efforts, apologising for the disruption and reiterating the commitment to decisions made based on professional judgement.

21st September 2022 – The Critical Site Incident is stood down. A long tail of recovery persists, with some clinical systems and data remaining inaccessible after this period.

6. HOW DID THE DATA CENTRE FAILURES HAPPEN AND HOW DID THE TRUST'S RISK MANAGEMENT SYSTEMS AND APPROACH OPERATE IN THIS CASE?

Given the inter-related issues, this section of the report answers principal questions (i) and (ii) together.

Main findings:

- The failure of both data centres was precipitated by the heatwave that peaked on 19th July. Whilst the heatwave was clearly an event outside of the control of the organisation, it was widely predicted, and yet the preparation and mitigation by the organisation was evidently insufficient to prevent a major failure of core IT operating systems.
- The contingency for data centre failure at the Guy's and St Thomas' sites was mutual back-up between the two sites: should one data centre fail, the other would act as a real-time back-up. While this was a reasonable mitigation for many sources of failure, it was insufficient to respond to simultaneous failure of both data centres. Given the relative proximity of the two data centres, it could have been foreseen that an environmental cause, such as a heatwave, could affect the two data centres simultaneously.
- Following forecasts of the heatwave, preparations were put in place at the St Thomas' data centre to manually hose down the condensers of the cooling system to keep down the temperature. This was carried out, but after a delay due to a broken hose connector. No such preparations were made at Guy's hospital and, although manual cooling was attempted there on 19th July, it was also delayed by difficulty locating a water supply. Had preparations been made earlier, this delay could have been avoided.
- There had been previous concerns about the cooling systems at both data centres: the ventilation at St Thomas' was known to be sub-optimal, though significant mitigations had been put in place following a trip-switch activation during a previous heatwave. The Guy's data centre cooling system was approaching the end-of-life, though the manufacturer had confirmed earlier in the year that it was still just within its expected operating lifespan.
- It is probable that the age of the some of the technical equipment at St Thomas' data centre contributed to the catastrophic failure at that site. That centre failed despite not breaching the manufacturer's upper limit for operational temperature. Humidity may have been a further contributing factor, as this was recorded as falling below the recommended lower limit of 20%, which can increase the risk of electro-static discharges and damage. It has not been possible to ascertain precisely the relative importance of three probable factors that contributed to the St Thomas' data centre failure: (i) the age of some of the technical equipment (ii) low humidity and (iii) high temperature. It is likely to have been a combination of those factors.
- GSTT is investing significantly in the strategic Electronic Health Record 'Epic' implementation and decisions to run legacy IT infrastructure close to end of life were made in the context of the Epic implementation planned for April 2023. With hindsight, the Trust should have given greater weighting to investment in elements of legacy IT infrastructure that were approaching end of life regardless of the new Epic system.
- After investigation, there is no evidence to suggest that the partial transfer of data from the Guy's site to the St Thomas' site (part of the planned back-up contingency) contributed in any way to the failure of the St Thomas' data centre.

- The division of responsibilities for management of the data centres and their environments was complex and confusing, with multiple third-parties responsible for different elements of maintenance, monitoring and management. In some areas, the division of responsibilities between parties was not clear. This created vulnerability in the management of the data centres, and in particular in preparation and response to an extreme weather event.
- There is no evidence of any other cause or malicious act, such as sabotage or cyber-attack. However, there was an unrelated cyber-attack on national IT systems used in the NHS that separately affected the Trust part way through the episode.
- There was no single failure of risk management that led directly to the incident, but many of the factors that combined to cause the severe and prolonged outage were known issues. Had the Trust acted sooner to fix those issues, the severity of the incident might have been considerably reduced.
- The risk of a failure of data centres was identified within the DT&I departmental risk register, although not specifically associated with a heatwave. There was a historic risk referring to heat issues affecting the St Thomas' data centre but it was closed in January 2020 and merged with another risk. Following this, it was not deemed to be sufficiently likely, after mitigations, to be escalated to the Trust's corporate risk register, or to trigger more substantial mitigating actions/investments. Therefore, it did not trigger a discussion specifically focused on this matter with the Trust Board.
- As noted above, the primary mitigation – two separate data centres acting as backup to each other – was insufficient to deal with a major environmental risk affecting both centres simultaneously.
- Whilst risk registers, and those who manage them, cannot always predict and manage all conceivable risks, and there needs to be a substantial element of judgement applied in assessing risk levels, a heatwave was a predictable risk and large scale failure of the data centres could have been predicted to cause catastrophic impacts on the Trust's ability to provide healthcare. With the benefit of hindsight, we can conclude that this risk was insufficiently controlled, scored and escalated.

Establishment of data centres:

6.1 Two data centres underpin the IT systems for Guy's Hospital, St Thomas' Hospital and the Trust's community services. The Guy's data centre is situated on the ground floor of Borough Wing and was constructed in 2007. The St Thomas' data centre is located in a modular building near Gassiot House and was constructed in 2012. The IT infrastructure was updated in 2015/16 as part of the Strategic Data Centre programme. Separate data centres support the Royal Brompton and Harefield Hospitals' IT systems.

6.2 The two data centres at Guy's and St Thomas' were designed to act as back-ups for each other, in the event that one failed. The two data centres employ a real-time back up service called Zerto that provides snapshots of server images between data centres, supplemented by an overnight back-up service called Commvault.

Responsibilities:

6.3 Responsibility for management of the data centres is divided between the Trust's DT&I Directorate and ATOS, the outsourced data centre management partner, as follows:

- **Data centre space and environment** - the DT&I Technical Space Team are responsible for providing physical space, power and managing all environmental aspects needed to host the services, aligned to industry best standards;
- **Air conditioning** - Outsourced by DT&I to SecureIT, who sub-contract to Flaktgroup (the manufacturer). SecureIT provide four service visits a year with three condenser cleans and other maintenance such as filter changers; and
- **Compute, storage and network equipment** - Responsibilities are split between DT&I and ATOS, as set out in a detailed service description. ATOS are responsible for notifying the Trust of unusual events relating to the functioning of the equipment. Remote monitoring for some hardware elements is further sub-contracted from ATOS to third parties (e.g. remote monitoring for the Netapp hardware is undertaken by Netapp through a third-party contract via ATOS). ATOS is responsible for "identifying any service or stability risks associated with the extended life of [the Trust's] infrastructure". ATOS are responsible for patching and updating software as required.

6.4 The service specification that sets out the responsibilities for the Compute, Storage and Network equipment is part of the contract for hosting of the new Electronic Health Record – Epic – that is planned to go live in April 2023. This contact was signed in 2020 and covers hosting for the pre and post Epic equipment. The main element of the tender bid for the 2020 contract relates to the future plan to move all Epic related systems to ATOS hosting (through a combination of cloud and on-site), post go-live.

Data centre cooling arrangements:

6.5 The Guy's data centre is cooled by four Denco air conditioners, with air circulated from condensers on the Cunliffe Laboratory roof nearby. The air handling units were installed in 2006 and are based on older technology than the units at St Thomas', although they have been subject to some upgrades and replacements. The original specification for the air handling units has not been located, though SecureIT state they were designed for an ambient temperature of 32°C, but are capable of operating above the design temperatures for short periods of time. In March 2021, SecureIT advised that these cooling devices were reaching the end of their life expectancy in 2021/22. SecureIT subsequently revised this to 2022/23.

6.6 A Request for Funding form to replace the Guy's data centre air conditioning was completed on 11th March 2022 by the DT&I Telecoms Infrastructure Manager, requesting £195k inclusive of VAT from the DT&I backlog maintenance fund. The request was moving through the normal internal review process prior to the incident, but had not been approved by 19th July. The request has since been increased to £360k and approved.

6.7 The Guy's data centre had coped effectively with previous high temperature events (e.g. 37°C on 31 July 2018, 38°C on 25 July 2019, 36°C on 7th August 2020) without any evidence of difficulty.

6.8 The St Thomas' data centre is also cooled by four Denco cooling units, with air circulated by condensers with fans located on an external wall, opposite the entrance to the data centre in the Gassiot House undercroft. The location of the condenser fans was acknowledged as not ideal, as there is a high degree of recycling of exhaust air, however there was no other location deemed to be practical. As a result of the sub-optimal location, the condensers were upgraded from the original design to deliver increased air flow and the units are specified to operate in up to 45°C ambient temperature.

6.9 In 2018, additional measures were taken to improve data centre cooling, based on a report by SecureIT that was carried out in response to a unit tripping out in high temperatures. This report recommended additional mitigations, including relocating the condensers to a new location. An application was made to the Essentia planning team but the proposed location at the entrance to the car park was needed to support the Covid response and the request was withdrawn while the additional mitigations were put in place. These mitigations were:

- increasing the aperture size of the security mesh, allowing greater exhaust air flow;
- insertion of cowling around fans to reduce flow upwards; and,
- installation of a large extractor at the entrance to the undercroft to improve removal of hot air.

6.10 Following these mitigations, the St Thomas' data centre coped with other high temperature events without further problems. For example, no issues were reported during the following ambient temperatures: 37°C on 31st July 2018, 38°C on 25th July 2019, and 36°C on 7th August 2020.

6.11 On Thursday 14th July 2022, the Trust was alerted to the impending high temperatures expected the following week. On Friday 15th July, the Telecoms Infrastructure Manager (within DT&I) sent a group email to the infrastructure team, instructing them to monitor temperatures in the data centres and informing them that there may be a need to hose down the condensers at the St Thomas' data centre site. Hosing the condensers with cold water is the only reliable way to improve the effectiveness of the condensers during periods of high-ambient temperature. The email did not reference the Guy's data centre because there had not been temperature-related issues at the Guy's site previously. Due to the known air flow limitations because of the positioning of the condensers, the St Thomas' data centre was seen as the priority for action to mitigate the heatwave risk.

Data centre failures:

6.12 On 19th July 2022, the high temperatures that day caused the air conditioning units at the Guy's data centre to overheat. Pressure in the condenser units increased, causing trip switches to activate and resulting in the units failing. Subsequently, at 14:16 that day, the temperatures inside the data centre reached over 50°C. Cold water, via a hosepipe, was applied to the external condensers located on the roof of Cunliffe Laboratories. To reduce the likelihood of damage to the infrastructure housed in the Guy's data centre, DT&I staff, working with ATOS, began a controlled shutdown of the equipment. Despite efforts to shut all equipment down in a controlled manner, some components providing network connectivity overheated and stopped working.

6.13 At the same time, the performance of the condensers was impacted by the high temperatures at the St Thomas' data centre. The cooling systems at this site did not fail altogether, but the temperature in the data centre did rise over the course of the day. Cold water was applied to external condenser units to cool them but, despite this, the temperature within the St. Thomas's data centre peaked at 36.2°C. This was approximately 15°C above the normal operating temperature, but within the operating temperature range for the installed equipment. At 14:01, sensors in the data centre reported that the relative humidity had dropped below the recommended 20% threshold, increasing the risk of electrostatic discharge and damage to equipment.

6.14 The NetApp Storage Area Network within the St Thomas's data centre had been in place since 2015/16 and was approaching end-of-life. At 14:22, components within one of the SANs at the St. Thomas' data centre began to fail. Despite attempts by staff from DT&I and ATOS to resolve these issues, additional storage components failed that afternoon and evening, resulting in a catastrophic failure of the St Thomas' data centre. The manufacturer, NetApp, was contacted by ATOS to investigate the SAN failure and to understand if data on the SAN could be recovered. The catastrophic failure of the St Thomas's storage array meant significant elements of the data centre were physically damaged and could not be recovered without the use of specialised recovery services.

6.15 As the Guy's data centre began experiencing issues, DT&I staff developed a plan to transfer application services to the St Thomas' data centre that afternoon, which was consistent with the risk mitigation plan for one data centre failing. However, the failure of the SAN at the St Thomas' centre meant DT&I staff were not able to execute their initial plan to recover some of the Guys' data centre systems onto the SAN at St Thomas'.

6.16 The Guy's data centre began to cool and a core network switch was restarted at 15:17. The data centre had cooled by 17:20. DT&I immediately commenced the recovery of the supporting network and computing infrastructure.

6.17 During the first 48 hours of recovery, effort focused in two key areas:

(i) recovery work on the St Thomas' SAN. This recovery work was initially the focus of DT&I and ATOS. The rebuilding of disks was protracted and did not progress as expected, due to additional disks failing within the Redundant Arrays of Inexpensive Disks (RAID) during the rebuild process. Each array was built using 20-22 disks. The tolerable disk failure within an array is a maximum of two disks. With support from NetApp (the manufacturer) work continued to attempt to resolve the issues, and

(ii) recovery work at both the Guy's and St Thomas' data centres to return telecommunications and the core network to operation. This required interaction with ATOS and the DT&I network team to resolve ATOS connectivity to the equipment they managed. This was followed by the recovery of supporting compute infrastructure at Guy's data centre back to operation prior to restoring services. The recovery was complicated by key servers, which enable use of the wireless network and staff remote access, being unavailable on the failed SAN at St Thomas'. Work was completed on recovering these service components to an alternative data store in the St Thomas' data centre. The Guy's data centre was operational by 09:15 on 20th July. The recovery was complicated when it was discovered that important supporting documentation to guide the recovery was stored on one of the servers at the St Thomas' SAN that had been damaged and was therefore initially inaccessible.

Trust risk management:

6.18 GSTT adopts a standard approach to the quantification and management of risks, scoring them based on a combination of likelihood and consequence. Individual risks are given a score out of five for each, and the multiple of these two ratings is what determines the overall risk score. Each risk is given a pre-mitigation score, and a post-mitigation score (i.e. the residual risk rating once mitigations are in place).

6.19 Data centre risks are the primary responsibility of DT&I. These are recorded on Datix as required by the Risk Management Policy. A risk management group for DT&I has been in operation since March 2019. The Trust Risk and Assurance Committee is responsible for escalating risk onto the Corporate Risk Register (CRR). The CRR is reviewed by the Trust Executive Committee. The Board is responsible for the Board Assurance Framework (BAF) which captures the Trust's key strategic risks.

6.20 Data centre resilience does not feature on the BAF or the CRR. The risk of data loss due to a cyber-attack has been on the CRR since January 2020. This has remained at a score of 16 (likely/major). As at the date of the incident, there were 23 DT&I open risks. There is no specific reference to air conditioning failure or high temperature risks in the current IT open risk register. There is a closed risk which relates to the overheating of the St Thomas' data centre and was added to the departmental register on 24th July 2018, following the air conditioning unit tripping out in high temperatures. This risk was initial scored as 20, likely/catastrophic, and was then reduced to 10 following the mitigations described above. The risk was then closed in January 2020 and 'amalgamated' with four other risks.

6.21 '*Risk of loss of key clinical systems due to failure of network equipment'* was opened in January 2020 and was scored 15, possible/catastrophic. The mitigations mainly concern the network upgrade project. Specific mitigations associated with heat are not described. DT&I risks scoring 12 or above were monitored by the Trust Risk and Assurance Committee in February 2020, and the Trust Risk and Assurance Committee agreed this risk should be managed within DT&I rather than escalated to the Corporate Risk Register.

6.22 While the redundancy provided by two data centres mitigated the risk of failure at an individual site, in order to have prevented the IT incident, the Trust needed to identify and effectively mitigate risks that could have simultaneously taken down *both* data centres.

6.23 The Trust Internal Audit team has reviewed the Corporate Risk Registers of a number of NHS organisations and none had a risk recorded specifically associated with a loss of air conditioning or extreme temperatures. All featured cyber security as the primary IT risk.

6.24 Risks with a very low chance of occurring but genuinely catastrophic impacts are sometimes referred to as 'black swan' risks, and will not usually be picked up and managed effectively through traditional risk management processes. One of the actions the Trust has taken since the IT incident is for the Board to consider its approach to the management of 'black swan' risks. Whilst the simultaneous failure of both data centres may have been a low probability event, the heatwave (and the potential impact on data centres) was predictable, and yet the Trust risk and governance mechanisms failed to prevent the IT outage of 19th July.

6.25 The Trust maintains a Hot Weather (Heat Wave) plan that has been regularly updated, most recently in June 2022. This plan brings together advice from the UK Health Security Agency and NHS England and describes 5 Heatwave alert levels (0-4) and a set of actions that need to be taken at each level. The plan sets out that at Level 1 – defined as summer preparedness which runs from 1st June to 15th September – DT&I has a responsibility to *'Check resilience of IT systems to ensure they can cope at higher temperatures'*. There are no further actions set out relevant to IT infrastructure at higher alert levels.

Root causes of data centre failures:

6.26 The initial cause of the data centre failures was the unprecedented high ambient temperatures experienced in London on 19th July, with recorded temperatures up to 40°C. Other data centres in London also experienced issues on this date, with both Google and Oracle reporting outages in London. However, the severity of the outage and the duration of the recovery period at GSTT appears to have been unparalleled. After investigation, this review has concluded that the drivers of the severity and duration of outage were the following factors:

- **Air Conditioning Design** – The location of the condensers for the St Thomas's data centre was not optimal, with a high degree of recycling of exhaust air in the Gassiot undercroft. This was a known issue and mitigations were in place, but despite these mitigations, temperatures in the data centre still climbed significantly above normal operating temperatures on the 19th July.
- **Delays in cooling the condensers** – Earlier action to cool the condensers by hosing with cold water could have kept the temperature in the data centres lower and prevented failure. Preparations had been made in advance of 19th July to hose down the condensers at the St Thomas' site. However, problems with a hose connector meant this was delayed and not as effective as it could have been. At Guy's, no such preparations were made and there was some initial confusion on the day about the availability of water supply on the roof of Cunliffe Labs. Preparing the hose and checking the water supplies could have allowed manual cooling to start earlier and reduced the risk of air conditioning failure.
- **Ageing equipment** – The air conditioning units that failed at Guy's data centre were approaching end of life and this may have contributed to their failure. Components within the St Thomas' Storage Area Network were at or approaching end of life. The manufacturer of the data Storage Array Network used at St Thomas' has suggested that the ageing of the St Thomas' SAN could have contributed to the catastrophic failure of the data centre, despite the environment remaining within the theoretical temperature operating range.
- **Management of the St Thomas' Storage Array Network** - The manufacturer of the St Thomas' SAN - NetApp – conducted a review of the reasons for the failure and identified three contributing causes for SAN failure, set out below with commentary:

- **Disks in the array that exceeded the recommended operating lifetime.** The Trust has been unable to confirm the age of the disks within the array (noting that it is time the disk has been in operational use that is relevant, rather than the date from production);
- **A version of the ONTAP software that was in use may have been missing a bug fix.** This is subject to ongoing consideration; and
- **The number of disks within the RAID groups had increased the probability of a multiple disk failure.** The SAN in the St Thomas' data centre had 20-22 disks per array, which technical documents confirm is within the acceptable number. Recovery is only possible where a maximum of 2 disks have failed, so the higher the total number of disks the greater the chances of more than two disks failing. This review has not found that this was a material factor.

- **Redundant back up failure** – As both data centres suffered failures at the same time, the real-time back-up solution did not function as planned. This meant that it was not possible to maintain live systems, by moving data and processes from one data centre to the other. Furthermore, the recovery plans were compromised when the real-time back-up solution ended up in a 'problem state' and could not be recovered without manual intervention (more information in Chapter 8, on the Trust's response). Data centre resilience was based on each data centre acting as a backup for the other, but as both data centres were located less than two miles apart they were exposed to the same environmental conditions simultaneously. There was no real-time back-up solution in place for a scenario where both data centres failed simultaneously.
- **Complex and confusing responsibilities** – Responsibility for cooling the data centre environment sat with DT&I rather than with Essentia who had responsibility for cooling the majority of the GSTT estate. Management responsibilities within the data centres were split between DT&I and ATOS, with monitoring for some key hardware elements further subcontracted to third-parties. This complex set of responsibilities may have led to some confusion relating to:
  - responsibility for upgrading software and identifying ageing equipment that needed replacing;
  - preparing for extreme environmental conditions;
  - raising and responding to issues and alerts regarding the data centre operations; and,
  - the level of technical system knowledge required for disaster response and recovery, noting that ATOS staff required technical direction by DT&I staff when managing system shutdown in Guy's data centre.

6.27 No data was stolen or accessed by malicious third-parties during the incident. Although the real-time Zerto back-up did not function perfectly on 19th July, as both data centres went down simultaneously, those elements of the St Thomas' data centre storage array that were not covered by Zerto had been backed up using the fall-back solution (Commvault) on 18th July. Therefore, the possible extent of data loss is limited to the eleven data storage components of systems that failed in the St Thomas' data centre, and only for data changes in the 24 hour period between the most recent Commvault back-up and system failure on 19th July. Elements of the failed SAN were sent off-site to a forensic recovery company, who are imaging the disks to try and recover this data.

6.28 The Trust notified the Information Commissioner's Office (ICO) of a data breach on 2nd August. The ICO initially wrote to the Trust on 31st August, having decided the case required further investigation, with a list of 16 questions, including a request for copies of any internal investigations reports regarding the incident. The Trust responded to the ICO questions on 14th September, answering those questions and sharing plans to review the incident, with a commitment to share the review report when it is finalised. The Trust received a further set of ICO questions on 28th October and replied on 18th November. In December 2022 the ICO informed the Trust it had closed its investigation with no regulatory action required.

Recommendations:

1. **The Trust should put in place a strategic plan, backed by appropriate investment, to ensure future computer processing, data storage and backup & recovery capabilities are robust in the face of expanding demand and resilient to foreseeable risks. This plan should conform to industry best practice and seek to optimise resilience and cost with a blend of cloud and onsite hosting.**
2. **Accountabilities and responsibilities for management of GSTT's data centres and other mission critical systems should be reviewed, clarified and, if helpful, simplified.**
3. **The Trust should make a general recommendation to NHS England to consider writing to other NHS Providers, alerting them to the specific risk of extreme weather-related IT failure and asking them to develop mitigations for this specific risk, learning generalised lessons from this report.**
4. **During preparation for future expected critical incidents (including weather events), the Trust should consider the age of infrastructure when assessing risk of failure and putting mitigations in place.**
5. **The Trust should maintain a register of assets nearing end of life and use this data to guide prioritisation of capital investment for backlog maintenance and equipment replacement for IT, medical equipment and estates assets).**
6. **Where mitigations are planned for critical infrastructure, during future extreme weather events (and other applicable critical incidents), the EPRR team should encourage dry-run practice of mitigations, to ensure equipment is appropriate and available, so mitigations can be implemented quickly. Mitigations should be planned for all critical infrastructure, not just those where issues have been known in the past.**
7. **The Trust risk management team should evaluate whether the current risk management framework is effectively managing and appropriately escalating risks which are low in probability but catastrophic in impact, and whether periodic external review of how the Trust is managing potentially catastrophic risks would be helpful.**
8. **The Trust should commission regular external reviews to provide assurance that the IT infrastructure underpinning key clinical and operational systems is being well managed and that any risks are appropriately mitigated.**

7. DID ANY ACTUAL OR POTENTIAL HARM COME TO PATIENTS BY OMISSION OR COMMISSION OF CARE?

Main findings:

- The Trust's first duty is to protect the safety of the patients under its care and its staff. It is a matter of the deepest sorrow and regret that any harm has come to patients by the failure of the Trust to maintain the function of its core clinical IT systems during the period in question. The Chief Executive issued, and reiterated, a full and heartfelt apology on behalf of the Trust and its Executive Team for the impacts on patients, staff and partners.
- A substantial Harm Review exercise has been commissioned, with an external, expert Chair, to ascertain whether any harm came to patients by omission or commission of care as a result of the IT outage. Given the scale and complexity of that undertaking, the Harm Review is ongoing and is expected to conclude by the end of 2022.
- No deaths or instances of severe harm relating to the outage have been identified to date. Two deaths were flagged by the Medical Examiner as requiring further examination to determine if they were potentially linked to the outage. After further investigation, these have subsequently been determined not to have any connection to the outage.
- One instance of moderate harm has been identified, which concerned a patient who was unable to have a transplantation when donor organs became available. One of the organs was able to be transplanted into another patient elsewhere but the other organ was not. The Trust's duty of candour to this patient was undertaken. This patient has subsequently had a successful transplantation.
- To date, 20 instances of low harm have been identified, which are all short-term delays in care or minor medication/transcribing errors due to the IT outage.
- The Trust's South East London system partners (acute trusts, primary care and ambulance service) are undertaking their own review and have not identified any instances of patients coming to harm.
- The Harm review remains open and will continue until all reconciliation of paper to electronic health records and all necessary actions (such as follow-up appointments being booked) have been undertaken.
- It is possible that further instances of patient harm will be identified at a later date, as patients present for medical treatment. A mandatory data field has been added to the Datix incident recording system to identify where any instance of harm may be potentially related to the IT incident. Should any future instances of potential harm come to light they will be investigated and reported through the established clinical governance processes to the Quality and Performance Committee and the Board, as appropriate.

7.1 This critical incident had an enormous impact on the operational running of the Trust. It is of paramount importance that the Trust finds and responds to any harm that may have come to patients as a result of the incident and that it acts now to prevent any harm in future. To that end, the GSTT Clinical Harm Review was commissioned to investigate the impacts of the incident on patients.

7.2 Ensuring the Harm Review is independent and transparent is essential. To ensure objectivity in the review, it is chaired by an external, independent expert: Dr Jane Fryer, Medical Director at NHS England

London region. The Trust review is complemented by a South East London System Harm Review that is also looking at any potential harm to patients redirected to other SEL providers, or any patients receiving care at other SEL providers linked to GSTT systems.

7.3 The objectives of the Harm Review are to:

- establish whether any harm has come to any patient as a result of the IT outage;
- identify any learning for the system;
- ensure the 'Duty of Candour' has been undertaken where harm has occurred; and,
- determine, as best as possible from the data available, if any patient groups have been disproportionately affected.

Methodology:

7.4 The Harm Review methodology ensures a pro-active and reactive approach to identifying all potential harm that is relevant to the IT outage. The review is not relying solely on incident reporting, and is proactively investigating for incidents of harm. Whilst the Trust has a positive reporting culture, and a system to report incidents on paper was established early within the IT outage, the reporting rate did reduce during this time period.

7.5 *Incident Analysis*: A link on the incident reporting form was established as a mandatory field for staff to select if an incident was linked to the IT Outage. This enables swift identification of these incidents. All reported incidents are reviewed within clinical directorates and should a case be identified that was linked it will be escalated as the teams review the harm. If the harm is judged as 'moderate or above', the clinical directorate will hold review meetings to discuss the incident and suggested investigation level. This is normal process and how serious incidents are identified on a regular basis. Monitoring and review of these incidents has occurred from 19th July to 30th September 2022 (by which point the majority of clinical systems had been restored). It is clear that further incidents may be identified in the future and these will be reviewed and actioned as per normal reporting and investigation processes. Any serious harm will be reported as a serious incident, in line with the national process.

7.6 *Complaints and harm identified*: The Trust has used complaints as a monitoring method in case a patient or carer/family has raised a concern and provided feedback to the Trust that was not reported as an incident. These are reviewed to determine if any caused harm and, where harm is found, will be followed up to ensure the incident is reported and included in the harm figures.

7.7 *Mortality Reviews*: The Medical Examiners review all deaths and, where they are suspected to be linked to the IT Outage, they will flag to the Trust mortality lead who will ensure clinical teams complete a Structured Judgement Review. This will include *all* deaths (even where there is no suspicion of a link to the outage) between 19th July and the end of September. Following this timescale, the usual process of death reviews will continue and any cases where there are concerns that actions or lack of actions had a significant impact on care will be reported and followed up as a serious incident.

7.8 *Unplanned Critical Care admissions*: Unplanned critical care admissions from 19th July to 31st August are being reviewed to identify if any admission due to patient deterioration was as a result of the IT Outage. A deeper review of a sample of cases (30% sample size) is being undertaken. It will be increased up to 100% as necessary if any harm is identified.

7.9 *Outpatient Reconciliation of Records*: All patients between 19th July and 31st August attending, or planned to attend, an outpatient appointment have been reviewed to ensure they have been re-booked for an appointment or, if they attended, that there is a clear outcome documented following the appointment. The outcome could be, for example, the booking of a follow-up appointment or blood test. This process

will ensure that all patients have had a review to ensure they were not missed whilst the systems were unavailable.

7.10 *Inpatient Reconciliation of records*: All inpatients from 19th July to 31st August are being reviewed to ensure there is a clear discharge summary sent to their GP. This will ensure the outcome of their inpatient stay, medication required and any next steps for follow up treatment are followed up.

The following is a brief summary of the definitions of harm, used in the Trust normally and through the Harm Review:

Low harm - any unexpected or unintended incident that required extra observation or minor treatment and caused minimal harm to one or more persons.

Moderate harm - any unexpected or unintended incident that resulted in further treatment, possible surgical intervention, cancelling of treatment, or transfer to another area, and which caused short-term harm to one or more persons.

Severe harm - any unexpected or unintended incident that caused permanent or long-term harm to one or more persons.

Death - any unexpected or unintended event that caused the death of one or more persons.

Findings so far:

7.11 Two deaths were flagged by the Medical Examiner as being potentially related to the incident. Both deaths have been further investigated and there was found to be no connection to the IT outage.

7.12 There is no evidence, to date, demonstrating that any patient group has been disproportionately affected. This will be re-visited at the conclusion of the Harm Review when all patient harms can be analysed against protected characteristics, as listed in the Equalities Act.

7.13 From 19th July to 30th September 2022 there were 166 incidents reported that were linked to the IT Outage, out of a total of 5,726 incidents in that period.

- One was reported as moderate harm: a pancreas transplant could not proceed, when an organ became available, due to safety concerns. Staff were unable to safely monitor critical observations without delay, such as blood results, post-surgery. One donor organ was reallocated to another patient but the pancreas could not be used. The planned recipient was informed of the cancellation, the 'Duty of Candour' was discharged and the patient has since had a successful transplant operation.
- There were 20 low harm incidents reported and these were reviewed (description, investigation and outcome) individually to confirm the harm level was correct and identify any areas of risk. All 20 were either confirmed as 'low harm' or could have been de-escalated to 'no harm' based on the investigation details. All incidents were either minor medicines errors or minor delays in diagnostics/results impacting care. Examples of low harm incidents include:
  - a delay in follow-up to an MRI report, which was identified two weeks later and actioned;
  - omitted medicine;
  - a delay in internal referral for hand splint, following surgery;
  - a delay in community care, for insulin administration, due to failed referral;

- a delay to community care potentially resulting in a pressure ulcer – actions were put in place as soon as the community visit took place;
- a delay to treatment of a pressure ulcer; and
- a number of incidents concerning misfiled documentation, delayed or lost referrals (all identified later), and missing records.

- 145 incidents were assessed as 'no harm', where the most common category was 'Appointment not made' (16 instances). Other examples in this category include: medication/transcribing errors; or delays in care from diagnostics or referrals.

7.14 The ten most common incident categories reported during the IT outage in 2022 are very similar to those reported prior to the IT outage (as part of standard annual reporting). 'IT related issues' saw a small increase in 2022 (0.6%) as the category of note most applicable to the downtime. The proportions of 'no harm' and 'low harm' incidents were similar and within expected range (98.0% in 2021; and 97.35% in 2022).

7.15 The SEL Integrated Care System Harm Review group includes King's College Hospital NHS Foundation Trust, Lewisham and Greenwich NHS Trust, South East London Primary Care representatives and London Ambulance Service. These system partners have reported that, so far, they have found no evidence of harm coming to patients elsewhere in the sector, as a result of the GSTT IT incident. The SEL Harm Review Group is awaiting the final inputs from the GSTT Harm Review to complete its report.

7.16 The Independent Harm Review Group chair has determined that the GSTT Harm Review will continue until there is complete reconciliation between paper and electronic records, care escalations have been analysed and SJRs have been completed into all patient deaths prior to the end of September. The target of reconciliation (paper notes uploaded to electronic records and actions completed) is higher than the level of reconciliation the Trust normally operates, which is 92-95% during business-as-usual operational running. Given the severity of the IT incident, the Harm Review Group chair has determined the Trust should apply the highest standards of rigour possible in this review, aiming for 100% reconciliation and where this may not be possible, the Trust has agreed to provide clear rationale on exception and mitigations.

7.17 As part of the wider review, the GSTT Head of Patient Experience has assessed the impact of the IT incident on patient experience, based on responses to the Trust's local survey programme during the four-week period from 18th July to 19th August. Volumes of feedback were lower than usual, as the mixed methods approach used by the Trust to capture feedback was impacted by the incident. However, some key themes have emerged:

- the impact of the IT incident was referenced most by adult patients attending for day case procedures and outpatients appointments;
- many of the issues raised by patients were amplifications of the issues raised by GSTT patients prior to the incident. For example, waiting times in clinics or challenges patients faced contacting the Trust by phone or email;
- a number of patients commented on the fact that staff could not access their records when they attended clinic; and
- many patients commented positively on how well staff appeared to cope in the face of the challenge and that they continued to deliver a good standard of care. Patients particularly valued being kept informed of delays and when staff made calls to reassure patients that appointments would go ahead.

"The appointment system had broken down and the lack of information was frustrating. The voice box was full so I was unable to leave a message, emails went unanswered."

"In spite of a huge IT outage the staff all appeared to pull together to present the best service possible, all staff encountered were friendly and helpful"

- Anonymous Patients' Feedback

7.18 The Trust has reviewed patient complaints to identify any episodes of harm. From 19th July to the end of September, there were 14 complaints received that are directly linked to the IT outage. Findings from the 14 complaints have not identified specific harm, although there is clear and understandable frustration. The complaints concern the following:

- one cancelled chemotherapy treatment, which was rearranged immediately;
- cancelled appointments and inability to reschedule during the outage; and,
- a lack of communication from the Trust to patients.

Recommendations:

9. **The Quality and Assurance team should maintain the additional field that has been added to the Datix risk recording systems so that should any patients present in the future with harm that could have potentially been related to the IT incident it can be investigated appropriately.**
10. **The Quality and Assurance team should refresh the audit of complaints, six months after the incident, to ensure that there is not a long-tail of relevant complaints that could form part of the Trust's learning from the incident.**
11. **While any incidents of harm are deeply regrettable, acknowledge the extraordinary work of GSTT clinical teams who delivered high volumes of activity throughout the incident without access to clinical records in a largely safe and effective manner.**
12. **As far as possible with the data available, complete assessment of whether any patient groups, especially those with protected characteristics as listed in the Equalities Act, were disproportionately affected by the IT incident.**

8. HAS THE TRUST FULLY UNDERSTOOD THE IMPACTS ON ITS STAFF SO THAT THEY CAN BE SUPPORTED APPROPRIATELY?

Main findings:

- The Trust's many thousands of staff have had a very challenging two years during the period of the pandemic and have performed exceptionally well, with unshakeable commitment to high quality patient care throughout that time.
- Coming towards the end of this incredibly difficult period, the IT outage has been a major blow to morale and to the confidence of staff in the Trust's ability to provide a reliable, digitally enabled healthcare environment.
- Many clinicians were placed in entirely invidious positions during the period of the IT outage, having to make complex, risk-based judgements on the basis of delayed or incomplete information. It is a testament to their skill and expertise that the hospitals and community services were able to continue caring for patients, and functioning to the extent they did, during the loss of core IT systems.
- The stress placed on clinical decision makers and others during this period cannot be under-estimated. Whilst some clinicians reported being comfortable working on paper, for the majority this was overwhelmingly a negative experience, especially for those that were unfamiliar with paper working.
- The Executives of the Trust made it clear that clinical decision makers would be supported in their professional judgements in line with standards of clinical practice.
- There have been many episodes recounted about staff members being on the receiving-end of patients' understandable anger and frustration due to the IT outage, for reasons that were outside of staff members' control. Again, this is a matter of the deepest regret for the Trust, which must continue to provide all reasonable support, including the provision of counselling and psychological support for any staff who need or may benefit from it.
- It should be acknowledged that, due to the timing of this incident, an important cohort of those staff affected - from amongst the Trust's junior doctors - rotated out of, or into, the Trust in the midst of the episode. The Trust should make all reasonable efforts to reach those who rotated out to ensure that the heartfelt apology has been heard and to offer support, if any is required, as a result of the IT incident.
- A crucial part of the future resilience and improvement of the Trust's clinical IT will be the implementation of the major new Electronic Health Record system, Epic. The Trust will need to work hard in the period ahead, particularly in the run up to, and beyond, the Epic go-live in April 2023 to rebuild the confidence of staff in its ability to manage IT systems safely and effectively.

Report from the Trust's Freedom to Speak Up Guardian

Sections in Italics represent anonymised quotes from staff:

"Staff at GSTT worked through the years of the pandemic and dealt with the subsequent backlog of demand without any hesitation or respite despite the fact that resilience was low and exhaustion widespread. Against that backdrop the IT systems failed at Guy's and St Thomas' on 19th July 2022.

At first there was confusion over the extent of the issue, staff feedback included: '*we were just really confused'; [working from home]'I put it down to my home connection issues. I couldn't get through to IT'; 'There was very mixed and limited information available,'*

'I don't know if someone could have done a walk around... Maybe they did that in clinical areas I don't know but we were in an office, so we were just really confused.'

Confusion was replaced by the dawning realisation that this was more than a minor computer glitch: *'The impact was massive; it seriously affected us'; 'We all knew very quickly that it was pretty catastrophic'*

Staff experienced the full gamut of emotions, they described feelings of anger, helplessness and frustration. *'I just felt useless'; ''It was awful - this experience has increased the likelihood that I will leave the NHS early'; 'It would be scary to have this type of situation again. We don't know what assurance is in place. There must be something in place for immediate action that this will not happen again.'*

The incident highlighted the paramount importance of clear, accurate and relevant communication. Staff needed both assurance that patients were safe and guidance available on when the systems would be restored. Trust-wide emails were abundant. Although long and detailed, they lacked relevant local information, which should have been better cascaded to the staff by managers.

Together with wider challenges faced today, the cost of living increases and continued demand for our services, the IT incident has undoubtedly been a blow on a bruise to the already-tested resilience of our staff. The psychological and wellbeing support available to staff, expanded during the pandemic, is needed today as much as it ever has been."

"It was a really frustrating time and we spent far too long "normalising" the situation. Everyone knew a heatwave was coming so I really don't understand why this happened. I personally found this situation embarrassing."

"It was astonishing how people stepped up, as they always do, but it's depleting on a personal level"

- Anonymised Staff Members

8.1 The skill, expertise and professionalism of the staff at GSTT are the organisation's lifeblood. They have provided incredible care over a long and extremely challenging two and a half years of the pandemic. The IT incident occurred at a time when the Trust was beginning to recover from Covid, and the difficult working conditions created by the IT outage have been a significant blow to the morale and energy of staff.

8.2 Strenuous efforts have been made in the course of this review to hear from as many staff as possible who wished to express their views on the IT incident. The Trust has put in place a range of different forums and easily-accessible communication channels for staff to share their views and experiences. In addition to the Freedom to Speak Up Service, the Trust set up a dedicated email inbox (ICTincidentreview@gstt.nhs.uk) for staff to share any concerns, information or feedback. Trust-wide communications were issued, setting out the approach to learning lessons from the incident and providing details of how staff could get in touch. An invitation to get involved in the review has been included in the staff bulletin regularly since September 5th (an example communication in Annex C). The review process was proactively taken to key staff forums and meetings, including staff-side engagements and Governors' meetings. The Freedom to Speak Up Guardian hosted a series of online staff forums, alongside the staff well-being psychology team, which were open for staff to share their experiences in a confidential and safe space.

8.3 As a result of the IT outage, for several weeks after the failure of the data centres, clinical staff were unable to access clinical IT systems. This included electronic patient records, investigation booking and results, clinical imaging and outpatient letters. This clearly had a profound effect on the ability of clinical staff to deliver care as they would reasonably expect. Some systems appeared to be initially unstable when they came back online. For example, shared files on File Explorer became available and then appeared to be missing which affected the confidence of staff in the restored systems.

8.4 Without access to patient records, staff were reliant on clinical histories from patients and relatives. Whilst important, staff were well aware that these histories can miss essential information. As a result, staff were left in the position of making clinical decisions on the basis of potentially incomplete information. At times, this could have included information that had serious safety considerations. It was unacceptable for the Trust's clinical decision makers to have been put in the invidious position of having to take difficult, risk-based judgements with inadequate information, when compared with their normal expectations of a modern healthcare environment.

> ***"It was a very stressful way to come to work. Practically we were disabled, we are highly dependent on IT, and were already exhausted from the pandemic and trying to catch up with the back-log."***
>
> ***"Many nights I cried due to the pressure and worry that I was missing something but as a senior clinical staff member I had to remain optimistic in front of colleagues and patients."***
>
> - Anonymised Staff Members

8.5 The Trust leadership sought to mitigate this pressure on clinical decision-makers by writing to clinical colleagues on 5th August and 23rd August, reassuring them that the Trust would collectively support their professional judgements taken in line with standards of clinical practice. . The full letters are in Annex D and extracts are below:

> ***"We are very mindful that some colleagues may have concerns about the fact that clinical decisions have had to be made during this period using different processes from those we are used to, and without the support of our usual systems. As the senior clinical leaders at the Trust, we want to reassure you that you have our full support and commitment to the decisions you have made and continue to make based on your professional judgement in-line with your standards of clinical practice."***
>
> Letter dated 5th August from Professor Ian Abbs, CEO;
> Avey Bhatia, Chief Nurse; and Dr Simon Steddon, Chief Medical Officer.

> ***"We understand that colleagues may continue to have concerns regarding the clinical decisions made during this period, particularly the use of different processes from those we are used to, and without all the clinical and other key information stored within electronic health records. As the senior clinical leaders in the Trust, we want to reassure you that you continue to have our full support and commitment to the decisions you have made and continue to make based on your professional judgement in line with your standards of clinical practice."***
>
> Letter dated 23rd August from Professor Ian Abbs, CEO;
> Avey Bhatia, Chief Nurse; and Dr Simon Steddon, Chief Medical Officer.

8.6 Nevertheless, the delivery of normal clinical activity was significantly more challenging and stressful than is usual or acceptable. The critical incident is likely to have had a significant psychological and emotional impact on some staff. The review heard a range of personal accounts from staff describing the impact the IT outage had on their ability to deliver care as they would expect, how the response was delivered, and frustrations with the pace of IT system recovery.

8.7 Non-clinical systems were also unavailable during the outage, which created a number of challenges for different cohorts of staff. For example, Trust payments to outside suppliers were disrupted which had multiple impacts such as community staff being unable to renew parking permits; the Trust was unable to issue new ID badges; and on-line training for new starters was unavailable. This had an impact on inducting new members of staff.

8.8 Frontline staff, clinical and non-clinical, were also asked to manage a lot of the understandable frustration and uncertainty experienced by patients. Without access to electronic records, clinics took place without the full background, and patients were routinely left recapping elements of their history that they would expect the Trust to know. Patients were also disappointed when test results were not available. Frontline staff had to manage this and reassure patients, despite having no responsibility for, or control over, the outage. This added to the stress that staff experienced, working through the period of the outage.

8.9 One such example of this was reported by a clinical member of staff. The patient arrived expecting to continue with their ongoing treatment and when told this was not going to be possible that day because of the IT outage, they became agitated and refused to leave. The member of staff managed the patient for a significant length of time while attempting to reach the patient's consultant by phone. The consultant reassured the patient who agreed to then leave. This is one example among many difficult experiences across the Trust.

8.10 The switch to working on paper created a range of challenges for staff. Some were more familiar with the processes than others and it was particularly stressful for those who were unfamiliar. This was a particular issue when junior doctors rotated through the Trust. The rotation brought a number of staff, unfamiliar with the Trust or the paper processes, into the organisation midway through the incident.

8.11 Another key theme from staff feedback is about the Trust communications regarding the incident. While initial internal communications took place before there was any external coverage of the incident, a number of staff reported that they heard about the incident from social media or the press before they heard through Trust communications channels. Others felt the Trust communications initially under-played the severity of the issue and would have liked to see an earlier apology from the Trust.

"Over the first days, some people seemed to be aware of certain information and others didn't; many of us had wildly varying experience of internet access, and access to emails, and we circulated advice as best as we could between ourselves but it was very ad hoc"

"The impression amongst the clinical team was in that the first few days the crisis was undermanaged, departments left on their own to figure things out and that there didn't seem to be communication of a coherent plan. This improved as the incident progressed."

- Anonymised Staff Members

8.12 It is worth noting that a good portion of the feedback from staff praised the resilience and flexibility with which teams on the ground responded to the challenges of the outage. Several staff highlighted the teamwork and personal efforts of colleagues during the incident and recovery phase. Others noted that teams were able to adapt quickly to work on a paper-manual way of working. Finally, some staff were pleased that managers were visible and supportive in clinical areas. This is to the further credit of the staff at GSTT and a mark of the commitment, adaptability and professionalism with which they handled the incident.

8.13 The efforts of the IT team, who worked around the clock to recover critical IT systems under considerable pressure, should also be recognised. Owing to their specialist knowledge of the Trust's technology systems, a number of individuals were key to the recovery of the data centres and worked excessively long hours over many weeks. DT&I senior management put in place measures to look after the welfare of these staff during the response.

8.14 Similarly, the Trust should recognise the substantial operational and clinical efforts that were made to reconcile paper records and minimise the impact of the disruption on the elective recovery. Both of these efforts are critical in minimising the impact of the outage on patients and took significant effort from staff across the Trust.

8.15 The Trust gave all staff an extra day of annual leave allowance, in recognition of the IT incident, whilst acknowledging it was of modest recompense.

Recommendations:

13. **The Trust should continue to ensure that psychological and well-being support is made available to any staff who need it.**
14. **As part of business continuity planning the Trust should consider developing an escalation protocol for clinical decisions that need to be taken on the basis of incomplete information.**
15. **The EPRR and communications teams should consider whether better channels of staff communication can be implemented during the early period of incidents where communications have been disrupted, to ensure that all staff (including those working off-site) are notified and updated promptly.**

9. HOW EFFECTIVELY DID THE TRUST MANAGE THE INCIDENT RESPONSE?

Main findings:

- The Trust has substantial, recent operational experience of managing major and critical incidents, with well-practised Emergency Preparedness, Resilience and Response protocols and procedures. The EPRR command and control system was stood-up swiftly and effectively, though some concerns have been raised that 'incident fatigue' and unclear impacts of the damage to the data centres may have contributed to some delays in escalating a more substantial response.
- There was not a pre-agreed design for an incident response structure during a total IT outage and the precise design of the response had to be shaped in the early days of the recovery. This added a further layer of complexity to the initial response.
- The move to 'paper hospitals and services' was managed effectively, although lessons can be learned from the incident debriefs for how to do this more rapidly and smoothly, with greater supplies of forms and standard operating procedures more accessible, in case of future need.
- The technical recovery of IT systems took substantially longer than was anticipated at the outset, lasting several weeks before near complete restoration. Part of the explanation for this protracted recovery was the multiplicity of historic IT systems - some 371 separate systems - that had been layered upon each other over time. This situation was far from best practice and the Epic system will consolidate and replace a large number of these legacy systems to substantially improve resilience and simplicity.
- The degree of physical damage to the St Thomas' data centre, and the need to acquire additional data capacity for the recovery, also contributed to the length of time to recover. The concurrent, but unrelated, cyber-attack on the CareNotes and Adastra systems added further complexity to the recovery.
- The order of restoration also complicated matters. Disaster Recovery preparatory exercises had generated a preferred order for restoring IT systems. However, in practice, this order was not always possible, due to the way the systems interacted. On top of this, there was understandable pressure from clinical teams to prioritise specific systems based on immediate need.
- There is no doubt that staff in DT&I worked tirelessly around the clock, and with incredible commitment, to try to recover IT systems according to this clinical prioritisation. However, in engaging with staff as part of these reviews, the issue that caused greatest anger and frustration was the perception that it took the Trust far too long to recover the core IT systems.
- There was also some criticism heard from staff and local partners that the Trust's initial external communications either under-estimated or underplayed the significance of the IT incident in severity and probable longevity. Whilst this should be received with humility as fair criticism, there is no evidence that it was deliberate but more a product of the uncertain timescales at the outset of the critical incident and that it was not expected to last as long as it did.

9.1 In response to the IT Incident, a huge number of clinical and non-clinical staff worked heroically to deliver continued high-quality care to patients, despite the disruption. The Trust has well-developed critical incident and business continuity procedures and has had reason to implement them on many occasions in recent years, for reasons ranging from the Covid pandemic to national security events.

9.2 In considering the Trust's overall response to the IT outage, the review has reflected on three main aspects of the response: how the incident was managed, including the move to a paper hospital; the technical recovery of IT systems; and the communications to staff, patients and partners during the incident.

9.3 Widespread IT disruption began to be reported around 14:00 on 19th of July and by 15:00 a Critical Site Incident was declared and communicated to staff and NHS England. The technical recovery continued for several weeks, including the restoration of clinical systems and the attempted recovery of data from damaged components of the data centre SAN. Clinical systems were restored gradually over that time, with some read-only access preceding full access. By the end of August, the majority of functionality of clinical systems had been restored.

Managing the Incident:

9.4 During the incident, the Trust implemented a paper-based operating model ('Paper Hospital') to support clinical activity. This included paper-based investigation requests, prescribing and discharge summaries. Once clinical systems were restored, a process of reconciling paper records with the electronic records began and remains underway at time of writing.

9.5 The incident was organised through a command and control structure, with a Strategic Command Group overseeing the activity of a number of Tactical Command Sub-groups. The interaction of the clinical and technical recovery was supported by a Clinical IT Restoration Group. The incident response 'Gold Cell' – including the Chief Digital Information Officer, Chief Operating Officer, Chief Nurse and Chief Medical Officer – met daily. A critical site incident – the highest level of GSTT internal incident – was immediately declared, and a meeting took place with NHS England two days later discussing how to further escalate the event given the scale of impact.

9.6 The EPRR debrief heard there was some nomenclature confusion, as GSTT incident definitions vary slightly to NHS England's, and some frustration that the incident was not declared as a major incident – although a major incident is associated with casualties presenting at the Emergency Department from an external event. The incident was downgraded on 22nd August and stood-down altogether on 21st September

9.7 With a critical incident of this type, the Trust had to make difficult judgements to balance operational and clinical risk. To close the Trust to core emergency services and the most clinically urgent 'elective' services may have reduced operational pressure at GSTT but could have increased clinical risk for patients. Diverts may also have put other local providers at risk, as they managed increasing demand. In this context, the Trust agreed with system partners that the most appropriate balance of clinical risk was to divert patients with specific high-risk, time-critical specialist needs (Section 136 mental health patients, vascular, cardiac and transplantation emergencies) to other hospitals, but to maintain core emergency activity at GSTT. Services were selected for divert by clinicians, on the basis that numbers were manageable for receiving sites, infrastructure was already in place to receive them (for example, where patient admissions are rotated between sites), and staff still had access to clinical records at receiving sites.

9.8 There were also concerns in the EPRR debrief that the Trust initially underestimated the scale and longevity of disruption, accepting that decisions and actions can only be taken based on information known at the time. The EPRR debrief recommended improvements to some EPRR processes based on learning from the incident. In particular, these concerned the structure of the Strategic Command Group, the flow of information from that to the Tactical Command Group and the structure of incident responses given the new Trust Operating Model. Resourcing of incidents and accessibility of EPRR documentation were also cited in the debriefs as areas for improvement.

9.9 The Paper Hospital functioned effectively during the outage and patient care was able to continue despite the operational challenges, albeit at reduced levels of activity and with widespread delays. There were some specific points of learning about the 'Paper Hospital', which the Site Operations team will take forward for future events and integrate with Epic rollout. In addition, the debriefs identified that resource and physical space available for the coordination of the 'Paper Hospital' were not always felt to be adequate. The EPRR team have recommended that, during future incidents, there is a dedicated site for the 'Paper Hospital' to be coordinated from, separate from the incident coordination centre and the site managers' office.

9.10 Familiarity with processes and paperwork was cited regularly in debriefs as an issues. Many clinical staff had never worked in such a way before. The Site Operations team will consider whether more training about paper processes should be delivered or whether forms and paperwork could be redesigned to make them more accessible. Non-clinical staff were asked to work from home on the days of the heatwave to reduce the number of areas in which Essentia had to manage temperature control and to enable load shedding, if required. While this had a clear and sensible rationale, it meant that there were fewer non-clinical staff on site to be drafted in to support with the running of the 'Paper Hospital'.

9.11 The South East London ICS 'After-Action Report' reviewed the response to the outage across SEL ICS, including at GSTT. There were a number of findings that SEL ICS and GSTT will take forward. In particular, it found that:

"The Level 3 Critical Incident flagged a significant gap in Business Continuity guidance being no reference to the effects of heatwaves on data centres. Although GSTT had had fully assured EPRR plans for heatwaves, no concerns had been raised about data centre ventilation or cooling. Clearly this is not just an issue for GSTT and early learning re this issue was shared with the SEL system... The Level 3 Critical Incident required a shift to a paper-based system which impacted on the Trust and in particular on primary care."

9.12 Recommendations made by the After-Action Report have been added to the recommendations in this review. Of note, the ICS report found that "GSTT's response to the incident was exemplary and professional".

Recovering IT systems:

9.13 Six weeks is clearly far too long for a major hospital to be without access to core clinical IT systems. There were three main reasons that the recovery of IT systems took so long: firstly, to do with the multiplicity and complexity of those systems; secondly, the extent of the physical damage to equipment at St Thomas'; and thirdly, the finite bandwidth of the DT&I staff who had the technical expertise and knowledge of those systems to be able to effect the recovery.

9.14 The current 'IT system' is, in fact, a collection of 371 IT systems integrated together that support patient records, patient administration, clinical services and infrastructure (e.g. networking). From April 2023 Epic EPR will replace c.70 of these legacy systems supporting the core patient record, patient administration and clinical services for the majority of patient pathways.

9.15 After the IT outage, restoring functionality and maintaining the integrity and coherence across the Trust required that systems be restored in a specific sequence. Following a DT&I project in 2020, the Trust had developed an order for restoring IT systems. This order was attempted, but had a number of challenges:

- during the recovery, it was discovered that some of the systems had interrelations that had not previously been identified. This required them to be restored in a different order;
- the order of restoration for systems had been stored on one of the disks in the SAN that was damaged, making it difficult to access in the initial recovery period;

- urgent requests were being received from frontline teams to restore some services as a priority that differed from the pre-planned order of restoration; and,
- the damage to the SAN meant that some of the systems were much harder to restore than had been modelled in the exercise.

9.16 The recovery process for each service software application was formed of seven stages, including user testing and formal sign-off. A number of systems integrated through PIMS (the Patient Administration Service), meaning several systems had to be restored as read-only initially, until all connected services had been restored. Unless the systems were connected, data on different systems would have been out of synchronisation and further complicated the recovery.

9.17 The scale of the outage and damage to the data centres also increased the level of complexity of the recovery. This meant that a small number of DT&I staff, with intricate technical knowledge of the systems, were relied upon to guide the recovery. The Strategic Command Group felt that external technical support for the recovery would not be of value as external support would still end up bottle-necked at the capacity of these internal technical experts.

9.18 The nature of the damage to the St Thomas' data centre also prolonged the recovery. There was extensive physical damage to the SAN storage, the storage capacity of the Trust was greatly reduced and there was not sufficient storage space to progress the recovery. During recovery the Trust needed to acquire additional storage. NetApp, the manufacturer of the St Thomas' data centre, agreed to provide this free of charge (estimated value c.£1m). At the scale needed for the recovery, NetApp had to source specific hardware from a number of suppliers, import them to the UK and quality assure them, before delivering them to the Trust. This took c.4 weeks and contributed to the time taken to recover functionality, even though an interim storage solution (via SoftCat) was procured to allow some progress to be made on recovery.

9.19 The back-up product (Zerto) employed by the Trust was intended to provide real-time snapshots of server images between the two data centres. The simultaneous failure of the Guy's data centre and the progressive failure of the St Thomas' SAN left some of the back-up servers in a conflicted state, which could not be resolved by DT&I or ATOS. Zerto was contacted to troubleshoot and identified a work-around for the affected server groups. The solution was a time-consuming manual process of extracting and copying files, which meant the recovery took longer than planned.

9.20 The damage to the SAN also led to a concern about the integrity of the data stored on it. The review has confirmed that no data left the organisation: data theft or cyber-attack have been ruled out, and there is no concern about a breach of patient confidential data. However, there is a concern that physical damage to the SAN has led to the destruction of some data. Period off-site backups of the servers have been captured and restored, but there is concern about data recorded *after* the backup, but *before* the catastrophic data centre failure (a period of less than 24 hours). DT&I have identified 750 servers that were affected and 145 that were physically damaged. The damaged services have been sent to a specialist forensics company to try to extract as much data as possible from the disks. A risk assessment of these disks has identified five servers containing clinical applications and data; three servers for file-sharing, which *may* contain clinical or financial data; and three servers of operational data, the loss of which could impact contract monitoring and business delivery.

Communication during the incident:

9.21 The review heard a number of concerns about communication, particularly messaging in the early days of the incident, both from staff and partner organisations. Some staff felt that the communication in the early days of the incident downplayed the scale of the incident and the operational impact of the IT outage. Early assumptions were that systems would be restored in a matter of days, when in fact it ended up being several weeks. There is no evidence that there was a deliberate attempt to obscure the

situation, but rather a lack of understanding in the initial phase about the complexity and timescale of the recovery.

9.22 While the initial internal communications took place before there was any external coverage of the incident, some staff, particularly those working from home or in the community, reported hearing about the incident first via social media or local news. This left staff with a number of unanswered questions and concerns and led to speculation about the cause and scale of the outage. The incident had left the Trust unable to update the intranet (GTi) or desktop wallpapers, or to issue pop up communications alerts. Without these usual routes of communications to staff, the Trust was more reliant on the use of email and management cascade to share information.

9.23 Once the scale of the issue was more clearly understood, the Trust stepped-up communication to staff in frequency and proportionality. This included intranet pages once this technology was re-enabled, all-staff emails and all-staff briefings with the Chief Executive, Chief Digital Information Officer and other executives. Recognising the scale of the incident and the need from staff for regular updates, from the 26th of July to the end of August, the Chief Digital Information Officer issued daily updates on the recovery and held regular MS Teams briefings. There were regular updates at the weekly Senior Leaders Meeting, including extraordinary sessions added to specifically update on the Incident.

9.24 In the EPRR debrief, it was suggested that emailed Clinical Alerts were used too frequently and became overwhelming, such that staff may have ignored them and implemented their own local means of sharing updates. Despite this, some staff still reported feeling that they received too little information on the progress of recovery. In the EPRR debriefs, some staff suggested that, because of a scarcity of information initially on the situation, Tactical Command Groups became over-crowded with staff attending to hear updates. Early Tactical sessions were described as being more akin to 'Question and Answer' sessions than a vehicle for managing decisions and coordinating the incident.

9.25 A further concern from staff was the level of communication to patients. On 28th July the CEO issued a full and heartfelt apology on behalf of the Trust and its Executive Directors, and the Chief Nurse apologised to patients and staff in an interview with BBC London on the same day. The Trust's social media channels also issued updates on the disruption (over Facebook and Twitter). Despite this, some staff felt that patients had not been properly informed of the level of disruption, so frontline staff were left to communicate this to patients. This often meant difficult conversations with frustrated or uncertain patients.

9.26 Finally, there was a view from local healthcare partners that the Trust did not do as much as it could have done to communicate the scale of disruption to external partners. The After Action Report from the ICS stated that "*Communications from the Trust and ICB were 'not useful' in in the first couple of days in confirming the potential severity of the impact/scope of the incident, likely due to available information and initial understanding of the eventual impact*". There were concerns from partners that, as a result, they did not adjust to the disruption and patients, in turn, may have been adversely affected. The SEL ICS Harm Review, described above, found no evidence of harm to patients in the wider South East London System, but the Trust should take on-board the feedback and adjust communication to partners appropriately, during future incidents.

Recommendations:

16. **The EPRR and Site Operations teams should update Paper Hospital processes, building on learnings from this Incident and setting out how the Paper Hospital will be operationally coordinated and reconciled should a large number of IT systems go down.**

17. **The EPRR team should review Incident Response procedures, standardising incident definitions with NHS England and improving communication to staff and partners. In particular, EPRR processes should be adapted to make them as accessible and easy to use as possible, recognising that, while training can improve knowledge among staff, the high turnover of staff at the Trust means that there are always likely to be a significant portion of staff who are unfamiliar with Trust processes or EPRR protocols.**

18. **DT&I, with external partners, should continue to attempt to recover data stored on the damaged SAN and identify if any serious implications are discovered related to destroyed data.**

19. **The switch to Epic should reduce the likelihood of another catastrophic failure of this kind and speed-up the recovery in the unlikely event it does occur. However, the DT&I team should consider how a recovery from a catastrophic event, under Epic, might be delivered, over what timescales and how clinical input about prioritisation could be fed into recovery processes.**

20. **The Trust should undertake practice drills for IT systems recovery at appropriately spaced intervals, potentially including full outage practices. These drills, as well as this incident, should be used to refine the order of recovery for IT systems in the event of a significant outage.**

21. **As per the ICO, the Trust should continue to address gaps in the Trust's data protection training by chasing completion through senior management and increasing the number of face-to-face training sessions available to staff.**

22. **DT&I should maintain a detailed register of legacy IT systems and infrastructure and a map of their interconnections to reduce reliance on the knowledge of key individuals in future.**

23. **DT&I should ensure there are enough staff in the department with the appropriate specialist knowledge and understanding of the IT infrastructure to support a rapid recovery from any future IT incident without needing to rely on a small number of key individuals. This will be aided by the register of systems mentioned in the previous recommendation.**

24. **As per the SEL ICS After Action Report, Disaster Recovery guidance should be reviewed to include specific guidance to data centre risks, including location of servers and use of Cloud storage processes. Learning should be shared widely throughout both NHS funded organisations, including primary care, and wider.**

25. **The EPRR team and communications team should consider how communications during critical and major incidents can be optimised, including through close alignment of the communications team with the tiers of the EPRR command structures.**

10. WHAT OTHER ACTIONS SHOULD THE TRUST TAKE TO IMPROVE INFRASTRUCTURAL RESILIENCE TO POTENTIAL EXTREME WEATHER EVENTS IN THE FUTURE?

Main findings:

- GSTT should not view the heatwave on 19th of July in isolation. Extreme weather events are predicted to be more common in the future. In particular, there are predicted to be more days registering above 40°C in the future, and more volatile, wetter winters which, while generally warmer, will still have short, extreme cold snaps. The Trust must ensure that its digital and physical infrastructure is prepared for, and resilient to, these changing conditions.
- The current estate includes some specific focal points of risk, largely stemming from either ageing estate that is vulnerable to failure, or equipment that was not designed to operate in these new extreme temperatures.
- Some specific pieces of cooling equipment showed signs of difficulty during the heatwave this summer. They should be the priority for further investigation to understand if they need to be repaired or replaced.
- Beyond that, a programme of staged plant and infrastructure upgrades, undertaken over the next few years, would increase overall resilience and ensure the robustness of systems to withstand the more extreme weather patterns that are likely to come. A replacement programme of equipment and systems will need to be aligned with the estates masterplan development proposals and an overarching decarbonisation strategy. A detailed review of cooling loads and capacities should include the building fabric and the first step in any mitigation measures should be to reduce cooling loads using passive measures, such as improving building insulation and shading, for example.
- Cooling and ventilation systems should be replaced at the end of their lifespan with equipment that is designed to handle higher extreme temperature events. Electrical systems should ensure they have the requisite contingency in the event of failure. Heating systems, across the estate, are ageing and likely to need replacement but this should be part of a larger, holistic programme of work.
- Further investigation of some specific areas was recommended by our external contractors, including the suitability of water storage, the capacity of electrical systems, and the vulnerability of rooftop areas to water-pooling.
- Individual Managed Service Agreements across the Trust should be reviewed to ensure that accountability for resilience of infrastructure is clearly understood and measures are in place, either from the provider or the Trust, as appropriate, to mitigate risks posed by climate change. These arrangements should avoid unnecessary complexity and excess ‘hand-offs’ between third-parties.
- Given the critical nature of the facilities that GSTT operates, and the high impact of failure of any of the systems and infrastructure that serve them, it is imperative to address any potential weaknesses identified in a timely and pro-active manner.

10.1 Though the extreme heat of 19th of July was unusual and literally unprecedented in this country, reliable climate modelling suggests that these events will recur and become more common in future. One of the strands of the review looked at how GSTT can prepare for future extreme weather events. On the 5th August GSTT commissioned a report by a specialist independent design and engineering firm,

Arup. The investigation from Arup focussed on identifying infrastructural vulnerabilities to increasing average and peak temperatures; increasing rainfall levels; and potential extreme cold weather events, across the GSTT estate and infrastructure. The recommendations looked at the investment priorities for the next five years, considering extreme weather events up to 2050. All four main acute hospital sites were in scope.

10.2 Climate modelling, based on the Met Office's UK Climate Prediction Model, forecasts warmer, wetter winters and hotter, drier summers, with average UK warming by 2070, under the high-emission scenario, projected to be in the range 0.9°C to 5.4°C. This general rise in temperatures will lead to increased incidence of extreme temperatures. Historical and projected data suggest that the extreme temperature events of this summer are unlikely to become the norm but will happen periodically with the external temperature in London expected to exceed 40°C once every three years by 2050. Winter temperatures are also expected to gradually increase, although increases in heat will cause the weather to be more volatile, potentially providing occasional short periods of extreme cold. These cold periods are not expected to be any worse than historical cold snaps experienced in the last twenty years. Studies of rainfall patterns suggest that short intense periods of rainfall are increasing, impacting on the frequency and severity of surface water flooding.

10.3 There is heating plant across the GSTT estate that is reaching the end of its life, particularly at Guy's Hospital. Cooling plant ranges from 17 years old to only a few months old. The cooling water distribution system in Tower Wing (Guy's) is plastic and is suffering from material degradation, leading to frequent leaks. Domestic water tanks are installed on all sites to provide back-up storage in the event of mains water failure. The general condition of the tanks appeared to be reasonable.

10.4 Specific problems with cooling systems at all four sites were reported during the extreme temperature events over the summer. In some instances, temporary mitigations have been implemented, including hosing the condenser coils and shading chilling systems.

10.5 Electrical infrastructure was reviewed across the estate and it was noted that increased generator capacity is planned to be valuable at the St Thomas' site and the Harefield site. Funding approvals are being sought at both sites to expand the generator capacity. Both proposals are still at a very early stage and neither have been signed-off yet by the Investment Portfolio Board.

10.6 One of the issues raised in chapter 4, which is likely to have been contributory to the incident, was the complicated accountabilities for cooling the data centres, between DT&I, Essentia, ATOS and SecureIT. Arup were asked to consider the existing Managed Service Agreements (MSAs) and where they might pose a risk to the integrity of infrastructure. A bottom-up review of MSAs found gaps in the information and assurances being provided by third-parties, as well as inconsistencies in the level of information provided. This highlights a potential vulnerability of future failure of the systems under third-party control, and the subsequent impact to GSTT operations. Facilities Management teams have been instructed to follow up with all providers of MSA contracts, to ensure that an adequate and consistent level of assurance is obtained across the estate.

10.7 Arup reviewed the resilience of different parts of the existing infrastructure to extreme weather events. Most of the chillers across the site are air-cooled, which have an upper-limit operating temperature of 35°C. There have been five days in the last four years when temperatures have been above 35°C. As a general guide, older chillers (implemented before 2010) are likely to begin to fail at 35°C and then stop functioning above 40°C. Performance of newer devices should continue as normal up to 40°C, when performance will begin to degrade, with failure expected above 45°C. These figures will be affected by the state of repair, location, load etc. on each individual cooler. The majority of chillers

across the estate coped with the recent high temperatures, without problems. Water-cooled chillers are less effected by the ambient air temperature, and so can be made more resilient to high temperature events, although there were issues on 19th of July among some of the existing water-cooled chillers.

10.8 Arup recommended that the majority of coolers are likely to be able to cope with expected temperatures for the next five to ten years. As plant naturally comes to the end of its life, it can be replaced with equipment selected to cope with higher design temperatures. The Arup report recommended that Air Handling Units are purchased with an operating temperature up to 35°C to 40°C pending further design.

10.9 A number of critical areas and equipment are served by single chillers, with no standby capacity should that chiller fail. Recent NHSE guidance (HBN00-07) states that "[as well as ensuring critical] cooling systems have adequate arrangements to power them, *adequate redundancy within the system should be provided*."

10.10 Heating facilities should be prepared to handle volatile temperatures in winter, including periods of operating at maximum capacity. The age of the heating infrastructure was flagged as increasing the likelihood of failures of components in the future. Wholesale replacement of heating systems would need to be part of a phased master-plan. This risk has been highlighted by recurrent failures of the Guy's Hospital heating system, which has had planned and unplanned down-time on a number of occasions this year. Funding has recently been secured to undertake a survey of the pipework and management of the boilers at Guy's Hospital by a specialist in mechanical stress analysis, expansion and movement in pipework systems. This comprehensive review and analysis work will be completed by early December and will inform the options and mitigations to resolve the failing pipe joints and leaks open to the Trust to undertake repairs to provide resilience.

10.11 Water left standing above 20°C for sustained periods is at increased risk of *Legionella*. In 2020, GSTT regrettably had a cluster of three cases of *Legionella* infection, after which the Trust instigated a full internal review, installed point-of-use filters and delivered urgent works to the water supply system to prevent *Legionella*. The Arup report reviewed water storage infrastructure*,* given rising temperatures pose a risk of *Legionella* growth in warmer water storage. The report recommended a further risk assessment be carried out on all tanks, including a calculation of the average residence time of the water and a measurement of the temperatures of the stored water. It was also recommended that automatic monitoring of water temperatures be provided, linked to the Building Management System, to provide an alarm when desired water storage temperature is exceeded, and to give an indication of where remedial works are needed. The Water Safety Committee should take responsibility for delivering these actions and provide confirmation to the Board once they are completed.

10.12 While electrical systems are generally more resilient to temperature changes, there were a few specific points of risk identified. Paper-Insulated Lead Cables are often more susceptible to faults and damage through increased exposure to higher temperatures. Switchgear with automation can be susceptible to rising ambient temperatures as the electronics in controls modules are typically only rated to 45-degrees. While critical automation systems are often configured in redundant arrangements, failure of individual controllers can still have significant impacts on operations or available system resilience. The quality of ventilation at switchgear sites was variable across the site, with particularly poor ventilation at Guy's Hospital and St Thomas' Hospital sites.

10.13 Increasing ambient and peak temperatures are only likely to cause issues for transformers during (unrelated) equipment failure or maintenance resulting in all of the load normally supported by a

redundant system being fed through a single unit. This increase in load could result in overheat in turn causing the remaining operational transformer to trip out.

10.14 Generators are often also arranged with redundancy, which decreases the likelihood of a cascade of failures during peak temperature conditions (or during maintenance). This is the case for all GSST sites visited, except for Harefield, where there is an ongoing application to upgrade the generator provision to include a redundant generator as back-up.

10.15 During inspection, Arup noted areas where plant might be susceptible to flooding during periods of intense rainfall:

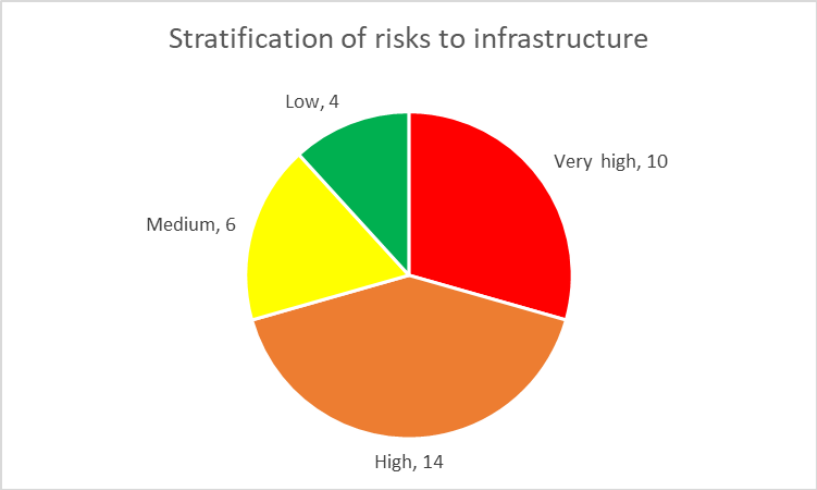
- St. Thomas' Lambeth Wing roof – some standing water was apparent around roof inlet gullies, which appeared to be blocked. In these areas there were several condensing units that were not mounted on plinths, which could be affected by local flooding;
- St. Thomas' North Wing roof – as above;
- Harefield Main block roof – Water was pooling around equipment, and local flooding had been experienced. Some of the condenser units would be vulnerable to this, and;
- Harefield services tunnel – Flooding had been experienced around medical air plant, with leak detection and a sump pump installed as a result.

10.16 Other instances of flooding, not mentioned in the report, have also been reported across the Trust. For example, recent flooding of the Surgical Innovation Centre of St Thomas' basement, due to leaves blocking drainage channels.

10.17 It was recommended that all roof areas are surveyed to identify potential issues with waterproofing of roofing membranes (as well as roof-mounted plant) that may be vulnerable to local flooding.

10.18 The Arup report compiled a risk register of systems and equipment that are likely to be affected by future climate change, with priorities for the next five years. This included indicative order-of-magnitude costs for replacement. This indicated a total investment of £25.3m spread over five years for all climate change-related replacements. These individual proposals are not currently part of the medium term capital plan (MTCP) but could form part of the proposal for a programme for infrastructure resilience, which is included on the MTCP.

10.19 Risks were scored by Arup on the basis of impact on staff and patients, operational impact, financial impact, reputational impact, and legal, quality and regulatory compliance. The scores for the risks were distributed as follows:



10.20 In conclusion, the age and suitability of the infrastructure across all four main hospital sites is variable. There were several examples of infrastructure that was at risk of failure because of age and a number of systems that had been designed to handle lower extreme temperatures. The Arup report injects a sense of urgency in recommending a phased investment programme to improve critical infrastructure resilience across the estate, such that action is taken now rather than reacting to the catastrophic failure of some engineering asset. Priority should be given to those specific pieces of equipment that showed signs of strain in the 19th July heatwave and these are highlighted in the report.

Recommendations:

26. Essentia should consider extending the review of infrastructure resilience to beyond the four core hospital sites, including community estate.

27. The Arup Report made a number of detailed technical recommendations to review the cooling, air handling, flood-prevention, water handling, electrical and heating infrastructure across the Trust (full list in Annex E). These recommendations should be prioritised within the backlog maintenance programme and an update provided to the Board by the Essentia Chief Executive.

28. Essentia and DT&I should complete the follow up with all providers of Managed Services Agreement (MSA) contracts, to ensure that an adequate and consistent level of assurance is obtained across the estate. An update should be provided to the Audit and Risk Committee about the outcome of this exercise.

29. In particular, it is recommended that a review is carried out of all domestic water storage across the sites to determine the current usage rates and storage capacities, to ensure these are optimal.

11. CONSOLIDATION OF MAIN FINDINGS:

11.1. How did the data centre failures happen and how did the Trust's risk management systems and approach operate in this case?

11.1.1. The failure of both data centres was precipitated by the heatwave that peaked on 19th July. Whilst the heatwave was clearly an event outside of the control of the organisation, it was widely predicted, and yet the preparation and mitigation by the organisation was evidently insufficient to prevent a major failure of core IT operating systems.

11.1.2. The contingency for data centre failure at the Guy's and St Thomas' sites was mutual back-up between the two sites: should one data centre fail, the other would act as a real-time back-up. While this was a reasonable mitigation for many sources of failure, it was insufficient to respond to simultaneous failure of both data centres. Given the relative proximity of the two data centres, it could have been foreseen that an environmental cause, such as a heatwave, could affect the two data centres simultaneously.

11.1.3. Following forecasts of the heatwave, preparations were put in place at the St Thomas' data centre to manually hose down the condensers of the cooling system to keep down the temperature. This was carried out, but after a delay due to a broken hose connector. No such preparations were made at Guy's hospital and, although manual cooling was attempted there on 19th July, it was also delayed by difficulty locating a water supply. Had preparations been made earlier, this delay could have been avoided.

11.1.4. There had been previous concerns about the cooling systems at both data centres: the ventilation at St Thomas' was known to be sub-optimal, though significant mitigations had been put in place following a trip-switch activation during a previous heatwave. The Guy's data centre cooling system was approaching the end-of-life, though the manufacturer had confirmed earlier in the year that it was still just within its expected operating lifespan.

11.1.5. It is probable that the age of the some of the technical equipment at St Thomas' data centre contributed to the catastrophic failure at that site. That centre failed despite not breaching the manufacturer's upper limit for operational temperature. Humidity may have been a further contributing factor, as this was recorded as falling below the recommended lower limit of 20%, which can increase the risk of electro-static discharges and damage. It has not been possible to ascertain precisely the relative importance of three probable factors that contributed to the St Thomas' data centre failure: (i) the age of some of the technical equipment (ii) low humidity and (iii) high temperature. It is likely to have been a combination of those factors.

11.1.6. GSTT is investing significantly in the strategic Electronic Health Record 'Epic' implementation and decisions to run legacy IT infrastructure close to end of life were made in the context of the Epic implementation planned for April 2023. With hindsight, the Trust should have given greater weighting to investment in elements of legacy IT infrastructure that were approaching end of life regardless of the new Epic system.

11.1.7. After investigation, there is no evidence to suggest that the partial transfer of data from the Guy's site to the St Thomas' site (part of the planned back-up contingency) contributed in any way to the failure of the St Thomas' data centre.

11.1.8. The division of responsibilities for management of the data centres and their environments was complex and confusing, with multiple third-parties responsible for different elements of maintenance, monitoring and management. In some areas, the division of responsibilities between parties was not clear. This created vulnerability in the management of the data centres, and in particular in preparation and response to an extreme weather event.

11.1.9. There is no evidence of any other cause or malicious act, such as sabotage or cyber-attack. However, there was an unrelated cyber-attack on national IT systems used in the NHS that separately affected the Trust part way through the episode.

11.1.10. There was no single failure of risk management that led directly to the incident, but many of the factors that combined to cause the severe and prolonged outage were known issues. Had the Trust acted sooner to fix those issues, the severity of the incident might have been considerably reduced.

11.1.11. The risk of a failure of data centres was identified within the DT&I departmental risk register, although not specifically associated with a heatwave. There was a historic risk referring to heat issues affecting the St Thomas' data centre but it was closed in January 2020 and merged with another risk. Following this, it was not deemed to be sufficiently likely, after mitigations, to be escalated to the Trust's corporate risk register, or to trigger more substantial mitigating actions/investments. Therefore, it did not trigger a discussion specifically focused on this matter with the Trust Board.

11.1.12. As noted above, the primary mitigation – two separate data centres acting as backup to each other – was insufficient to deal with a major environmental risk affecting both centres simultaneously.

11.1.13. Whilst risk registers, and those who manage them, cannot always predict and manage all conceivable risks, and there needs to be a substantial element of judgement applied in assessing risk levels, a heatwave was a predictable risk and large scale failure of the data centres could have been predicted to cause catastrophic impacts on the Trust's ability to provide healthcare. With the benefit of hindsight, we can conclude that this risk was insufficiently controlled, scored and escalated.

11.2. Did any actual or potential harm come to patients by omission or commission of care?

11.2.1. The Trust's first duty is to protect the safety of the patients under its care and its staff. It is a matter of the deepest sorrow and regret that any harm has come to patients by the failure of the Trust to maintain the function of its core clinical IT systems during the period in question. The Chief Executive issued, and has reiterated, a full and heartfelt apology on behalf of the Trust and its Executive Team for the impacts on patients, staff and partners.

11.2.2. A substantial Harm Review exercise has been commissioned, with an external, expert Chair, to ascertain whether any harm came to patients by omission or commission of care as a result of the IT outage. Given the scale and complexity of that undertaking, the Harm Review is ongoing and is expected to conclude by the end of 2022.

11.2.3. No deaths or instances of severe harm relating to the outage have been identified to date. Two deaths were flagged by the Medical Examiner as requiring further examination to determine if they were potentially linked to the outage. After further investigation, these have subsequently been determined not to have any connection to the outage.

11.2.4. One instance of moderate harm has been identified, which concerned a patient who was unable to have a transplantation when donor organs became available. One of the organs was able to be transplanted into another patient elsewhere but the other organ was not. The Trust's duty of candour to this patient was undertaken. This patient has subsequently had a successful transplantation.

11.2.5. To date, 20 instances of low harm have been identified, which are all short-term delays in care or minor medication/transcribing errors due to the IT outage.

11.2.6. The Trust's South East London system partners (acute trusts, primary care and ambulance service) are undertaking their own review and have not identified any instances of patients coming to harm.

11.2.7. The Harm review remains open and will continue until all reconciliation of paper to electronic health records and all necessary actions (such as follow-up appointments being booked) have been undertaken.

11.2.8. It is possible that further instances of patient harm will be identified at a later date, as patients present for medical treatment. A mandatory data field has been added to the Datix incident recording system, to identify where any instance of harm may be potentially related to the IT incident. Should any future instances of potential harm come to light they will be investigated and reported through the established clinical governance processes to the Quality and Performance Committee and the Board, as appropriate.

11.3. Has the Trust fully understood the impacts on staff so that they can be supported appropriately?

11.3.1. The Trust's many thousands of staff have had a very challenging two years during the period of the pandemic and have performed exceptionally well, with unshakeable commitment to high quality patient care throughout that time.

11.3.2. Coming towards the end of this incredibly difficult period, the IT outage has been a major blow to morale and to the confidence of staff in the Trust's ability to provide a reliable, digitally enabled healthcare environment.

11.3.3. Many clinicians were placed in entirely invidious positions during the period of the IT outage, having to make complex, risk-based judgements on the basis of delayed or incomplete information. It is a testament to their skill and expertise that the hospitals and community services were able to continue caring for patients, and functioning to the extent they did, during the loss of core IT systems.

11.3.4. The stress placed on clinical decision makers and others during this period cannot be under-estimated. Whilst some clinicians reported being comfortable working on paper, for the majority this was overwhelmingly a negative experience, especially for those that were unfamiliar with paper working.

11.3.5. The Executives of the Trust made it clear that clinical decision makers would be supported in their professional judgements in line with standards of clinical practice.

11.3.6. There have been many episodes recounted about staff members being on the receiving-end of patients' understandable anger and frustration due to the IT outage, for reasons that were outside of staff members' control. Again, this is a matter of the deepest regret for the Trust, which must continue to provide all reasonable support, including the provision of counselling and psychological support for any staff who need or may benefit from it.

11.3.7. It should be acknowledged that, due to the timing of this incident, an important cohort of those staff affected - from amongst the Trust's junior doctors - rotated out of, or into, the Trust in the midst of the episode. The Trust should make all reasonable efforts to reach those who rotated out to ensure that the heartfelt apology has been heard and to offer support, if any is required, as a result of the IT incident.

11.3.8. A crucial part of the future resilience and improvement of the Trust's clinical IT will be the implementation of the major new Electronic Health Record system, Epic. The Trust will need to work hard in the period ahead, particularly in the run up to, and beyond, the Epic go-live in April 2023 to rebuild the confidence of staff in its ability to manage IT systems safely and effectively.

11.4. How effectively did the Trust manage the incident response?

11.4.1. The Trust has substantial, recent operational experience of managing major and critical incidents, with well-practised EPRR protocols and procedures. The EPRR command and control

system was stood-up swiftly and effectively, though some concerns have been raised that 'incident fatigue' and unclear impacts of the damage to the data centres may have contributed to some delays in escalating a more substantial response.

11.4.2. There was not a pre-agreed design for an incident response structure during a total IT outage and the precise design of the response had to be shaped in the early days of the recovery. This added a further layer of complexity to the initial response.

11.4.3. The move to 'paper hospitals and services' was managed effectively, although lessons can be learned from the incident debriefs for how to do this more rapidly and smoothly, with greater supplies of forms and standard operating procedures more accessible, in case of future need.

11.4.4. The technical recovery of IT systems took substantially longer than was anticipated at the outset, lasting several weeks before near complete restoration. Part of the explanation for this protracted recovery was the multiplicity of historic IT systems - some 371 separate systems - that had been layered upon each other over time. This situation was far from best practice and the Epic system will consolidate and replace a large number of these legacy systems to substantially improve resilience and simplicity.

11.4.5. The degree of physical damage to the St Thomas' data centre, and the need to acquire additional data capacity for the recovery, also contributed to the length of time to recover. The concurrent, but unrelated, national cyber-attack on the CareNotes and Adastra systems added further complexity to the recovery.

11.4.6. The order of restoration also complicated matters. Disaster Recovery preparatory exercises had generated a preferred order for restoring IT systems. However, in practice, this order was not always possible, due to the way the systems interacted. On top of this, there was understandable pressure from clinical teams to prioritise specific systems based on immediate need.

11.4.7. There is no doubt that staff in DT&I worked tirelessly around the clock, and with incredible commitment, to try to recover IT systems according to this clinical prioritisation. However, in engaging with staff as part of these reviews, the issue that caused greatest anger and frustration was the perception that it took the Trust far too long to recover the core IT systems.

11.4.8. There was also some criticism heard from staff and local partners that the Trust's initial external communications either under-estimated or underplayed the significance of the IT incident in severity and probable longevity. Whilst this should be received with humility as fair criticism, there is no evidence that it was deliberate but more a product of the uncertain timescales at the outset of the critical incident and that it was not expected to last as long as it did.

11.5. What other actions should the Trust take to improve infrastructural resilience to potential extreme weather events in the future?

11.5.1. GSTT should not view the heatwave on 19th of July in isolation. Extreme weather events are predicted to be more common in the future. In particular, there are predicted to be more days registering above 40°C in the future, and more volatile, wetter winters which, while generally warmer, will still have short, extreme cold snaps. The Trust must ensure that its digital and physical infrastructure is prepared for, and resilient to, these changing conditions.

11.5.2. The current estate includes some specific focal points of risk, largely stemming from either ageing estate that is vulnerable to failure, or equipment that was not designed to operate in these new extreme temperatures.

11.5.3. Some specific pieces of cooling equipment showed signs of difficulty during the heatwave this summer. They should be the priority for further investigation to understand if they need to be repaired or replaced.

11.5.4. Beyond that, a programme of staged plant and infrastructure upgrades, undertaken over the next few years, would increase overall resilience and ensure the robustness of systems to withstand the more extreme weather patterns that are likely to come. A replacement programme of equipment and systems will need to be aligned with the estates masterplan development proposals and an overarching decarbonisation strategy. A detailed review of cooling loads and capacities should include the building fabric and the first step in any mitigation measures should be to reduce cooling loads using passive measures, such as improving building insulation and shading, for example.

11.5.5. Cooling and ventilation systems should be replaced at the end of their lifespan with equipment that is designed to handle higher extreme temperature events. Electrical systems should ensure they have the requisite contingency in the event of failure. Heating systems, across the estate, are ageing and likely to need replacement but this should be part of a larger, holistic programme of work.

11.5.6. Further investigation of some specific areas was recommended by our external contractors, including the suitability of water storage, the capacity of electrical systems, and the vulnerability of rooftop areas to water-pooling.

11.5.7. Individual Managed Service Agreements across the Trust should be reviewed to ensure that accountability for resilience of infrastructure is clearly understood and measures are in place, either from the provider or the Trust, as appropriate, to mitigate risks posed by climate change. These arrangements should avoid unnecessary complexity and excess ‘hand-offs’ between third-parties.

11.5.8. Given the critical nature of the facilities that GSTT operates, and the high impact of failure of any of the systems and infrastructure that serve them, it is imperative to address any potential weaknesses identified in a timely and pro-active manner.

12. CONSOLIDATION OF RECOMMENDATIONS

12.1 How did the data centre failures happen and how did the Trust's risk management systems and approach operate in this case?

12.1.1 The Trust should put in place a strategic plan, backed by appropriate investment, to ensure future computer processing, data storage and backup & recovery capabilities are robust in the face of expanding demand and resilient to foreseeable risks. This plan should conform to industry best practice and seek to optimise resilience and cost with a blend of cloud and onsite hosting.

12.1.2 Accountabilities and responsibilities for management of GSTT's data centres and other mission critical systems should be reviewed, clarified and, if helpful, simplified.

12.1.3 The Trust should make a general recommendation to NHS England to consider writing to other NHS Providers, alerting them to the specific risk of extreme weather-related IT failure and asking them to develop mitigations for this specific risk, learning generalised lessons from this report.

12.1.4 During preparation for future expected critical incidents (including weather events), the Trust should consider the age of infrastructure when assessing risk of failure and putting mitigations in place.

12.1.5 The Trust should maintain a register of assets nearing end of life and use this data to guide prioritisation of capital investment for backlog maintenance and equipment replacement for IT, medical equipment and estates assets).

12.1.6 Where mitigations are planned for critical infrastructure, during future extreme weather events (and other applicable critical incidents), the EPRR team should encourage dry-run practice of mitigations, to ensure equipment is appropriate and available, so mitigations can be implemented quickly. Mitigations should be planned for all critical infrastructure, not just those where issues have been known in the past.

12.1.7 The Trust risk management team should evaluate whether the current risk management framework is effectively managing and appropriately escalating risks which are low in probability but catastrophic in impact, and whether periodic external review of how the Trust is managing potentially catastrophic risks would be helpful.

12.1.8 The Trust should commission regular external reviews to provide assurance that the IT infrastructure underpinning key clinical and operational systems is being well managed and that any risks are appropriately mitigated.

12.2 Did any actual or potential harm come to patients by omission or commission of care?

12.2.1 The Quality and Assurance team should maintain the additional field that has been added to the Datix risk recording systems so that should any patients present in the future with harm that could have potentially been related to the IT incident it can be investigated appropriately.

12.2.2 The Quality and Assurance team should refresh the audit of complaints, six months after the incident, to ensure that there is not a long-tail of relevant complaints that could form part of the Trust's learning from the incident.

12.2.3 While any incidents of harm are deeply regrettable, acknowledge the extraordinary work of GSTT clinical teams who delivered high volumes of activity throughout the incident without access to clinical records in a largely safe and effective manner.

12.2.4 As far as possible with the data available, complete assessment of whether any patient groups, especially those with protected characteristics as listed in the Equalities Act, were disproportionately affected by the IT incident.

12.3 Has the Trust fully understood the impacts on staff so that they can be supported appropriately?

12.3.1 The Trust should continue to ensure that psychological and well-being support is made available to any staff who need it.

12.3.2 As part of business continuity planning the Trust should consider developing an escalation protocol for clinical decisions that need to be taken on the basis of incomplete information.

12.3.3 The EPRR and communications teams should consider whether better channels of staff communication can be implemented during the early period of incidents where communications have been disrupted, to ensure that all staff (including those working off-site) are notified and updated promptly.

12.4 How effectively did the Trust manage the incident response?

12.4.1 The EPRR and Site Operations teams should update Paper Hospital processes, building on learnings from this Incident and setting out how the Paper Hospital will be operationally coordinated and reconciled should a large number of IT systems go down.

12.4.2 The EPRR team should review Incident Response procedures, standardising incident definitions with NHS England and improving communication to staff and partners. In particular, EPRR processes should be adapted to make them as accessible and easy to use as possible, recognising that, while training can improve knowledge among staff, the high turnover of staff at the Trust means that there are always likely to be a significant portion of staff who are unfamiliar with Trust processes or EPRR protocols.

12.4.3 DT&I, with external partners, should continue to attempt to recover data stored on the damaged SAN and identify if any serious implications are discovered related to destroyed data.

12.4.4 The switch to Epic should reduce the likelihood of another catastrophic failure of this kind and speed-up the recovery in the unlikely event it does occur. However, the DT&I team should consider how a recovery from a catastrophic event, under Epic, might be delivered, over what timescales and how clinical input about prioritisation could be fed into recovery processes.

12.4.5 The Trust should undertake practice drills for IT systems recovery at appropriately spaced intervals, potentially including full outage practices. These drills, as well as this incident, should be used to refine the order of recovery for IT systems, in the event of a significant outage.

12.4.6 As per the ICO's recommendation, the Trust should continue to address gaps in the Trust's data protection training by chasing completion through senior management and increasing the number of face-to-face training sessions available to staff.

12.4.7 DT&I should maintain a detailed register of legacy IT systems and infrastructure and a map of their interconnections to reduce reliance on the knowledge of key individuals in future.

12.4.8 DT&I should ensure there are enough staff in the department with the appropriate specialist knowledge and understanding of the IT infrastructure to support a rapid recovery from any future IT incident without needing to rely on a small number of key individuals. This will be aided by the register of systems mentioned in the previous recommendation.

12.4.9 As per the SEL ICS After Action Report, Disaster Recovery guidance should be reviewed to include specific guidance to data centre risks, including location of servers and use of Cloud storage processes. Learning should be shared widely throughout both NHS funded organisations, including primary care, and wider.

12.4.10 The EPRR team and communications team should consider how communications during major incidents can be optimised, including through close alignment of the communications team with the tiers of the EPRR command structures.

12.5 What other actions should the Trust take to improve infrastructural resilience to potential extreme weather events in the future?

12.5.1 Essentia should consider extending the review of infrastructure resilience to beyond the four core hospital sites, including community estate.

12.5.2 The Arup Report made a number of detailed technical recommendations to review the cooling, air handling, flood-prevention, water handling, electrical and heating infrastructure across the Trust (full list in Annex E). These recommendations should be prioritised within the backlog maintenance programme and an update provided to the Board by the Essentia Chief Executive.

12.5.3 Essentia and DT&I should complete the follow up with all providers of Managed Services Agreement (MSA) contracts, to ensure that an adequate and consistent level of assurance is obtained across the estate. An update should be provided to the Audit and Risk Committee about the outcome of this exercise.

12.5.4 In particular, it is recommended that a review is carried out of all domestic water storage across the sites to determine the current usage rates and storage capacities, to ensure these are optimal.

13. ACKNOWLEDGEMENTS

The multiple strands of investigation and inquiry that have formed this review have required a huge amount of effort and tenacity from many people across the Trust and its partner organisations. They are too numerous to name individually, but what has been impressive from them all is the spirit of openness and self-reflection with which this review has been treated. Even when dealing with matters that are difficult and sensitive, I have not encountered defensiveness, but rather a willingness to understand, learn and improve, driven by deep regret about this incident and a determination that it should never be repeated.

I would like to give great credit and thanks to the senior working group that has driven forward this review and compiled the report and recommendations.

Whilst I cannot name them for the sake of preserving anonymity, most importantly of all, I would like to thank sincerely and give all due credit to the many staff from the Trust who contributed their experiences and views about this incident, some of whom did so, unforgettably, with tears in their eyes.

Lawrence Tallon, January 2023

14. GLOSSARY OF TERMS

ATOS – Private company responsible for managing the data centres.

Air Handling Unit – A device used to regulate and circulate air as part of a heating, ventilating, and air-conditioning (HVAC) system. Typically a large metal box, located on building rooftops, containing a blower, heating or cooling elements, filter racks or chambers, sound attenuators, and dampers.

Board Assurance Framework – Brings together in one place all of the relevant information on the risks to the board's strategic objectives

Corporate Risk Register - A mechanism to manage high level risks facing the organisation from a strategic, clinical and business risk perspective. The high level strategic risks identified in the CRR are underpinned and informed by risk registers overseen at the local operational level within Directorates.

DT&I – GSTT's in-house Data, Technology & Informatics Directorate.

Duty of Candour - This term means that every health and care professional must be open and honest with patients and people in their care when something that goes wrong with their treatment or care causes, or has the potential to cause, harm or distress.

EPIC – A new Electronic Health Record, which will be adopted by the Trust from April 2023. This will replace and consolidate a number of existing IT systems

Emergency Preparedness, Resilience and Response - This is a strategic national framework containing principles for health emergency preparedness, resilience and response for NHS-funded organisations in England including but not limited to NHS Trusts, Foundation Trusts, Care Trusts, providers of NHS-funded primary care, NHS commissioning organisations including NHS England and integrated care boards.

Essentia – GSTT's in-house estates and facilities management group.

Hosing Down of Condensers - Applying continuous cold water using a hose to the outdoor air conditioning condensers to cool their temperature.

Information Commissioner's Office - the UK's independent body set up to uphold information rights.

NetApp – Manufacturer of the data centre storage network equipment.

Redundant Arrays of Inexpensive Disks - a way of storing the same data in different places on multiple hard disks or solid-state drives (SSDs) to protect data in the case of a drive failure.

Secure IT – Third-party company responsible for servicing the data centre air conditioning.

South East London Integrated Care System – A partnership that brings together the organisations responsible for publicly funded health and care services in south east London, to make the greatest possible contribution to the health and wellbeing of people living in our six boroughs.

Storage Array Network - A Storage Area Network is a specialized, high-speed network that provides network access to storage devices.

Structured Judgement Reviews – A blended review comprising traditional clinical-judgement based review methods with a standard format. The objective of the review method is to look for strengths and weaknesses in the caring process, to provide information about what can be learnt about the hospital systems where care goes well, and to identify points where there may be gaps, problems or difficulty in the care process.

ANNEX A – Summary of the Terms of Reference

The summary of the Terms of Reference for the separate strands of the Review, as well as the external investigations, are as follows:

Strands	GSTT CNO and CMO led Harm Review	SEL System Harm Review	GSTT Internal Audit	GSTT IT infrastructure review	NHSE London IT Infrastructure Review	SEL System After Action Review	GSTT EPPR Debrief	GSTT Staff review	Estates review
High level objectives	- To establish whether any harm has come to any patient as a result of the IT failure/outage - To identify any learning for the system - To ensure Duty of Candour has been undertaken where harm has occurred	- To understand and assess the impact in terms of outcomes and harm for SEL patients as a result of the critical incident - To identify any further actions required to mitigate harm - To identify learning for the SEL system including recommendations as to the management of future system incidents	Examine the existing risk management processes within DT&I, specifically in relation to the two strategic data centres at the Guy's and St. Thomas' sites and identify how responsibility for the management of environmental risks has been allocated. This will require a review of the decision making concerning the establishment of the Strategic Data Centres and any contractual arrangements entered into since their establishment	To investigate the incident and recovery timeline and establish root cause. Recognise opportunities where lessons can be learnt and improvements made. - Identify the sequence of events that led to the IT failure - The recovery process deployed to restore services - Interactions between IT and EPRR - Review the business continuity plans to understand what was achieved in response to the major incident	- What happened: what detailed events that led to the failure of the data centres - Were there any prior actions / management decisions that contributed to the IT outage - What actions were taken to recover from the outage (detailed timeline and decisions re recovery process) - Why did it take so long to recover (weeks vs days) Do we have a sensible plan going forward	System EPRR after action review focusing on four questions: - What was expected to happen? - What actually occurred? - What went well and why? - What can be improved and how?	GSTTT EPRR debrief with the objectives to: - Compare what happened against existing disaster recovery and business continuity plans. - Highlight what aspects of the response worked well and what the Trust's successes were during the response. - Determine areas for improvement and what the Trust would do differently next time. - Document lessons identified to create a structured action plan to support organisational improvement.	Pull together the various sources of information we have across the Trust including in order to understand: - How the IT incident impacted on staff - How did we commuincate to and support our staff - How do our staff feel about the IT incident and the Trust's response - What more could we do to support our staff in future incidents	To look from a wider perspective at future resilience to deal with extremely high or low temperatures, flooding etc. that will arise as a consequence of the climate emergency. In addition, the data centre incident has highlighted a vulnerability where parts of our estate are managed by others (e.g. Managed Service Agreements). The review will look at these areas of risk and the assurance arrangements in place.
Timelines	3-4 months with a long tail Emerging findings end October	3-4 months with a long tail Emerging findings end October	12 weeks from start of September Emerging findings mid Sept / final report mid November	3 weeks from start September Findings late Sept	Findings early January 23	Seven week timeline Findings mid October	6 weeks post stand down Findings mid October	3 months Findings mid October	6 weeks timeline Findings mid October

ANNEX B – Incident Definitions

As defined in the NHS EPRR Framework, July 2022, for the NHS in England, there are three types of incident:

a. Business Continuity Incident – an event or occurrence that disrupts, or might disrupt, an organisation's normal service delivery, to below acceptable pre-defined levels. This would require special arrangements to be put in place until services can return to an acceptable level. Examples include surge in demand requiring temporary re-deployment of resources within the organisation, breakdown of utilities, significant equipment failure or hospital acquired infections. There may also be impacts from wider issues such as supply chain disruption or provider failure.

b. Critical Incident – any localised where the level of disruption results in an organisation temporarily or permanently losing incident its ability to deliver critical services; or where patients and staff may be at risk of harm. It could also be down to the environment potentially being unsafe, requiring special measures and support from other agencies, to restore normal operating functions. A Critical Incident is principally an internal escalation response to increased system pressures/disruption to services.

c. Major Incident – The Cabinet Office, and the Joint Emergency Services Interoperability Principles (JESIP), define a Major Incident as an event or situation with a range of serious consequences that require special arrangements to be implemented by one or more emergency responder agency. In the NHS this will cover any occurrence that presents serious threat to the health of the community or causes such numbers or types of casualties, as to require special arrangements to be implemented.

An incident is then described in terms of the level of response and coordination required. This level may change as the incident evolves (see Figure 1). They are specific to the NHS in England and are not interchangeable with other organisations' incident response levels.

Level 1	An incident that can be responded to and managed by an NHS-funded organisation within its respective business as usual capabilities and business continuity plans
Level 2	An incident that requires the response of a number of NHS-funded organisations within an ICS and NHS coordination by the ICB in liaison with the relevant NHS England region
Level 3	An incident that requires a number of NHS-funded organisations within an NHS England region to respond. NHS England to coordinate the NHS response in collaboration with the ICB. Support **may** be provided by the NHS England Incident Management Team (National).
Level 4	An incident that requires NHS England national command and control to lead the NHS response. NHS England Incident Management Team (National) to coordinate the NHS response at the strategic level. NHS England (Region) to coordinate the NHS response, in collaboration with the ICB, at the tactical level.

Figure 1: NHS incident response levels

GSTT also employ three types of incident, with the same definitions as the NHS EPRR Framework but with slightly different terminology.

- Serious site incident (comparable to business continuity incident)
- Critical site incident (comparable to critical incident)
- Major incident

There are also GSTT-specific levels which apply to these definitions with those for serious and critical site incident viewable in the table below.

Incident level	Examples of incidents	Action	Lead
LEVEL 1 Disruption affecting a single service but services maintained.	Routine staff sickness or absence levels	Service BCPs activated and managed at local level	Managers and team leaders

SERIOUS SITE INCIDENT			
LEVEL 2 2+ services affected. Operational difficulties but service delivered at acceptable level.	Disruption To: IT, premises or supplies, business as usual, serious staffing issues, MPS and firearms on site, potential loss of activity,	Service BCPs activated. Communication to affected areas of the Trust	Coordinated by SNP/PNP supported by DMT RBH SMoC lead linking with above
LEVEL 3 Potential negative impact on patients. May require support from other departments.	Prioritised activity disrupted, i.e. ED Ambulance redirect, diagnostics services, infection control, theatre, pandemic. Pressure surge management at Red	Trust BCP and control rooms may be activated Trust-wide communication	Coordinated by SNP/PNP supported by SMoC and DMT RBH SMoC lead linking with above
CRITICAL SITE INCIDENT			
LEVEL 4 Critical services affected for an unacceptable period of time. Must be declared to NHS01.	Fire in a ward, purple beds pressure surge, pandemic Coordination with external partners required or mutual aid needed	Trust BCP and Control rooms MUST BE activated	Command and Control activated. Led by Strategic Commander.

ANNEX C – Invitation to participate in the IT Critical Incident Review

The following text was taken from the daily Staff Bulletin email.

Let your voice be part of our IT critical incident review

Since the serious IT incident which began during the extreme weather in July, a series of internal and external reviews into the incident have been taking place. These cover a number of aspects including: the issues that led to the failure of the data centres; the impact on patient care; our post-event response including communications with patients, staff and other stakeholders; how we can build our resilience for the future; as well as the impact on you, our staff. Information on how you can contribute to these reviews is available on GTi (available here for colleagues at Harefield and Royal Brompton).

Eve Bignell, the Trust's Freedom to Speak Up Guardian, along with members of the staff psychological support team, are hosting 2 additional virtual listening events – confidential spaces for you to share how this incident affected you and your colleagues (please note, no personal details will be used as part of the review, and we will not be admitting new participants after 10 mins past the start time):

- Wednesday 16 November, 1pm to 2pm. Join via Microsoft Teams
- Monday 21 November, 1pm to 2pm. Join via Microsoft Teams

As well as hearing about the many challenges you have faced, we are also keen to discover if there were any positive outcomes from this incident, for example did communication across your team improve, were people more visible, or have there been any changes that you would like to keep?

Please note these listening events are about the Trust IT incident, not the separate national cyberattack impacting Adastra and Carenotes.

If you would like to share your experiences but are unable to attend or wish remain anonymous, please email speakup@gstt.nhs.uk from any email account you choose.

ANNEX D – Letters to staff on individual clinical risk

Chief Executive
St Thomas' Hospital
Westminster Bridge Road
London
SE1 7EH

Friday 5 August 2022

Dear Colleague

First, we wish to apologise again for the significant challenges you have experienced as a result of the recent and ongoing IT critical incident. We understand the tremendous difficulties you have faced in both caring for our patients and working with colleagues near and far, and remain extremely grateful for your outstanding efforts in continuing to provide the best possible care in these circumstances.

We are very mindful that some colleagues may have concerns about the fact that clinical decisions have had to be made during this period using different processes from those we are used to, and without the support of our usual systems. As the senior clinical leaders at the Trust, we want to reassure you that you have our full support and commitment to the decisions you have made and continue to make based on your professional judgement in-line with your standards of clinical practice.

Please do look after yourselves and each other, and if you do have any issues or concerns, please discuss these with your colleagues and your leadership team. If you have been particularly affected by some of the issues you have dealt with during this period please take the opportunity to access the Trust's health and well-being service as your welfare and wellbeing is our priority.

Once again, we are incredibly grateful and thank you for your continued compassion, resilience and determination at this challenging time.

Kind regards

Professor Ian Abbs
Chief Executive Officer

Avey Bhatia
Chief Nurse

Dr Simon Steddon
Chief Medical Officer

Professor Ian Abbs
Chief Executive
St Thomas' Hospital
Westminster Bridge Road
London
SE1 7EH

Tuesday 23 August 2022

Dear Colleague

We wanted to follow up the letter we sent clinical colleagues on 5 August, to reiterate our full support for the clinical decisions you and your teams are making as we continue to deal with Guy's and St Thomas' IT critical incident

We fully understand the significant impact this incident has had over an extended period of time. We also appreciate the additional challenges many of you are now dealing with as a result of the national issue with Advanced systems, namely Carenotes and Adastra.

We know that this national outage is having a major impact across our urgent care centres, dental services and most extensively in our adult and children's community services. We know that you are experiencing tremendous difficulties and we are extremely grateful for your outstanding efforts in continuing to provide the best possible care to our patients and each other in these circumstances.

We understand that colleagues may continue to have concerns regarding the clinical decisions made during this period, particularly the use of different processes from those we are used to, and without all the clinical and other key information stored within electronic health records.

As the senior clinical leaders in the Trust, we want to reassure you that you continue to have our full support and commitment to the decisions you have made and continue to make based on your professional judgement in line with your standards of clinical practice.

Please do look after yourselves and each other and if you do have any issues or concerns, please share with your leadership team. We are in frequent contact with all leadership teams and are keen to hear any ideas you have for how we can support you further.

Once again, we are incredibly grateful for your continued compassion, resilience and determination at this challenging time.

Kind regards

Professor Ian Abbs
Chief Executive Officer

Avey Bhatia
Chief Nurse

Dr Simon Steddon
Chief Medical Officer

ANNEX E – Detailed Recommendations from the Arup Report

It is recommended that these actions are taken forward by the Essentia Director of Engineering.

A replacement programme of equipment and systems will need to be aligned with the estates masterplan development proposals and an overarching decarbonisation strategy. A detailed review of cooling loads and capacities should include the building fabric and the first step in any mitigation measures should be to reduce cooling loads using passive measures, such as improving building insulation and shading.

1. Undertake a detailed review of air handling chillers across the estate that struggled in the extreme temperatures of the recent summer. Review siting to see if shading/ventilation can be improved, or if re-siting or replacement is necessary.

2. Assess the remaining chillers against the risk assessment to determine a priority schedule for replacement works and the siting/local environment of these chillers to determine any improvements that can be made, which might delay the need to replace.

3. Undertake feasibility studies of increasing the capacities of roof water cooling plant (cooling towers) and replacing cooling water distribution pipework (Guy's, Tower Wing).

4. The majority of the heating plant and distribution networks across the estate are in need of replacement. The practicalities of this work are complex, due to the far-reaching impacts on all buildings across the estate, and the need to decarbonise the heating networks to meet climate reduction commitments. There is however a pressing need to initiate a feasibility study into how this could be undertaken in a phased managed way, the cost, timescale and overall benefits.

5. Almost all the air handling coils are likely to need to be replaced with larger coils in order to cope with projected increasing external air temperatures. AHUs should be reviewed to determine if this can be done in-situ as a retro-fit. Where this is not possible, larger coils will need to be specified for replacement AHUs, as they reach the end of their lives. The report recommended that, as Air Handling Units need replacing, new ones are purchased with an operating temperature up to 35°C to 40°C pending further design (current operating temperature is 28°C).

6. Undertake a detailed capacity study of the electrical infrastructure at all sites to understand what is available should the loads increase. Use metering and trend logging of key electrical infrastructure to identify where equipment is operating close to its resilient capacity. Conduct thermal imaging of critical electrical infrastructure during peak periods to identify problems.

7. Review locations where PILC (paper insulated lead cables) high voltage cables are still in use and prioritise replacement as part of any adjacent/associated works or upgrades.

8. Review potential for upgrades to ventilation systems within fully enclosed transformer rooms which currently have minimal ventilation provision.

9. Install infrastructure to facilitate semi-regular 100% load 8-hour load bank testing on essential generator sets.

10. Conduct a detailed survey of PLC (hardware) and SCADA (software) control and monitoring systems to ensure critical controls equipment and associated battery systems are in a suitable temperature-controlled environment.

11. Undertake survey of all roof areas to identify potential issues with waterproofing of roofing membranes (incl. roof-mounted plant) that may be vulnerable to local flooding along with guttering and downpipe capacity to discharge excessive rainfall.