SHSCT IT Outage 17th September 2025

Incident Review Group

Incident Outcome Report

16th January 2026

Contents

1. FOREWORD BY INDEPENDENT CHAIR

It is a well-known fact that health and social care services are under constant and increasing pressure. Many of these pressures can be associated with an aging population, people living longer with complex and multiple conditions, leading to increasing healthcare needs, whilst at the same time, working within the constraints of a publicly funded health and care system. Health and social care services have finite resources both in financial and human terms, as a result, we need to find new and innovative ways to be more productive, reduce waste and look to transform what we do, and how we do it. In essence, not keep doing the same things better, but do better things. This type of transformation can include the use of digital data and technology, systems, and services.

However, as we become increasingly dependent on digital, data, and technology, we often only realise just how dependent we are when things go wrong, and the events of 17th September 2025 illustrates this challenge.

My role as the independent chair of this review has been to understand what happened and why, and at the same time, learn from this experience as both a health and social care Trust and equally as a partner in the wider health and social care system.

You will see from the following report that issues such as this are seldom straightforward, and are often multifactorial, usually a combination of; People, Process and Technology related issues converging to create the perfect storm.

The findings within this report have been guided by a commitment to excellence and integrity, as a result, I am confident that the root cause of the incident, the recommendations, actions and associated learning will strengthen the Trust's and wider system resilience and thereby improve the health and social care services for the people and communities we serve.

I would like to formally commend the Trust and its many healthcare and supply chain partners in the way this review has been conducted, which was always patient and service user focussed and implemented in an open transparent and cooperative manner.

Finally, I wish to express my gratitude to all those who have contributed their time and expertise to the production of this report. Their collaborative effort has been essential in achieving the high standard of analysis presented here.

Professor Graham Evans
BA(Hons), MSc, DProf, CEng, CITP, FBCS, FRSA, FCMI, MInstMC, MIET

2. EXECUTIVE SUMMARY

2.1. Background

This report summarises the findings of the independently chaired Incident Review Group in respect to the major incident arising from the unexpected Information Technology (IT) outage incident experienced by the Southern Health and Social Care (HSC) Trust (the Trust) on the 17th September 2025. The incident had an adverse impact on the operational services of the Trust, resulting in the cancellation of 1,647 patient appointments and the step up of an ambulance divert away from the Trust's two acute hospital sites.

In summary, an unplanned IT network outage prevented access and use of the organisation's digital and technology services. This included access to healthcare records and other business services from the Trust's internal local area network (LAN), however, Trust users could access IT systems through the use of other access points out-with the Trust's core technology infrastructure.

During the incident, the Trust, supported by its partners, quickly implemented business continuity plans in a controlled and coordinated manner, and governance systems and decision support processes all appeared to work with a high degree of effectiveness. As a result of the prompt actions of the Trust and its partners, the direct impact of the incident lasted only one business day, which, given its nature could have been far more service impacting.

Nonetheless, this has been an extremely regrettable event and the Trust conveys its sincere apologies to all of those impacted by the incident. Furthermore, the Trust wishes to assure patients, service users, and staff that it has prioritised its efforts to ensure that all findings and the rich learnings from the incident are captured and are being actively shared with the wider HSC.

Learning from this incident can and will place the Trust in a much stronger position going forward. As part of this independently chaired review, as well as understanding (and mitigating) the technical root cause of the incident, the review has sought to understand what went well and importantly what can be learnt in regard to all aspects of the incident response and the Trust's digital governance arrangements that could be further improved.

In reading this report it should be noted that the details contained within reflect the status of referenced information, such as appointment dates, incident reports, and complaints logs, as at the time of publication.

2.2. Approach

In taking forward this learning focussed review the Trust established a dedicated Incident Review Group (IRG), which was independently chaired by industry expert Professor Graham Evans, and comprised the Trust's Executive Directors of Medicine and Nursing, supported by four sub-groups. This structure has enabled a detailed review of the technical root cause of the incident to be undertaken, as well as a review the effectiveness of the Trust's emergency planning and business continuity structures and procedures and associated internal and external communications.

It should be noted that the Trust has not waited for the final reporting of this review exercise to commence the process of sharing and embedding the important learnings from the incident, with relevant regional learning already having been shared with other HSC Trusts and a number of early recommendations implemented.

2.3. Key Findings and Learnings

Following the successful restoration of network access at 16:15 hrs on 17th September, the Trust's IT team worked closely with the Trust's external network infrastructure support provider and its subcontractor (who provide technical assistance centre support to the Trust for all aspects of data centres and wider comms infrastructure) to forensically review system logs, and the timeline of events prior to and subsequent to the incident, with the intention of identifying the technical root cause.

Supported by IT colleagues from across the HSC namely, Western HSC Trust, Northern HSC Trust, the regional Business Services Organisation (BSO), and Digital Health & Care Northern Ireland (DHCNI), it was concluded that:

- the change control process associated with the planned upgrades to the Trust's data centres (DC1 and DC2) prior to the IT outage was considered appropriate and proportionate and the correct process and mandate had been followed by the Trust.
- the infrastructure in both data centres is considered to be highly resilient and correctly designed for its purpose.
- the root cause of the outage was as the result of human process error. Review of the detailed technical logs has identified that the outage occurred when a member of the network infrastructure support provider attempted to install the necessary software onto the data centre hardware - the configuration was mistakenly applied to the active data centre (DC1) which was running and not to the inactive data centre (DC2) which was being upgraded.

In learning from the incident, the Trust has already taken steps to strengthen existing processes and to significantly reduce the risk that a similar incident can happen again in the future. This includes ensuring "dual-engineer" oversight (a second pair of eyes) for work on critical infrastructure components, implementing the digital capture of such upgrade work, and proactively engaging the vendor technical assistance centre ahead of planned works to the Trust's core digital infrastructure.

In addition to the Technical Root Cause Analysis (RCA) sub-group findings outlined above, the other IRG sub-groups considered the effectiveness, learnings, and recommendations for improvement in respect to the following areas:

- ***Major Incident Response***, including general emergency planning and business continuity arrangements applied across the organisation;
- ***encompass Business Continuity Arrangements,*** being the business continuity and recovery procedures enacted in respect to the electronic patient record system (encompass) in the Trust; *and*

- ***Internal and External Communications*** both during and following the IT outage incident.

The key findings and lessons learned in respect to these areas are summarised in Section 6 of this report, along with the findings of a review of the Trust's digital governance arrangements. Section 6 also summarises the findings regarding the regrettable impact of the incident on patients and service users, summarising the number and type of cancelled appointments, the arrangements applied to reschedule the cancelled appointments, and wider feedback from patients and service users in respect to the incident.

2.4. Conclusions and Recommendations

Overall, the IRG findings conclude that the Trust, along with its HSC and technology partners, worked in a responsive manner to minimise the duration of the incident restoring services within one business day and demonstrating strong foundations in emergency planning, business continuity, and communications. Furthermore, clinical and operational teams delivered an outstanding, patient-first response, demonstrating exceptional professionalism and adaptability in activating business continuity plans and maintaining patient safety throughout the IT outage which must be commended.

However, the incident has highlighted opportunities to further strengthen preparedness, resilience, and communications, particularly during IT system outages. In this regard it is acknowledged that the implementation of the encompass patient record system in May 2025 has added a new aspect to the Trust's emergency planning and business continuity arrangements. Work continues to ensure this is fully embedded as a core element of the Trust's wider emergency and business continuity planning and preparedness.

The key recommendations identified by the IRG are summarised in Section 7 of this report and include improving technical safeguards for critical infrastructure upgrades; developing robust contingency communication methods that can be used in IT outage situations; enhancing IT resilience through mobile connectivity and hosting reviews; and ensuring adequate resources and equipment to maintain service continuity. Alongside the Trust's commitment to regular training, testing and exercising of the updated emergency management plans, implementing the identified recommendations will reinforce operational readiness and help reduce the risk and impact of any similar incidents in the future.

The Trust's Senior Leadership Team (SLT) is collectively responsible for assessing the recommendations outlined in this report and, in terms of next steps, will agree an action plan to consider their implementation.

3. BACKGROUND

This report relates to the IT outage incident experienced by the Trust at 08:05 hrs on Wednesday 17th September 2025. This full network outage resulted in a loss of connectivity for Trust staff to key clinical information systems including encompass (the electronic patient record system), the radiology & digital pathology system (NIPACS) and the laboratory information management system (LIMS). These systems remained accessible to all other HSC Trusts in Northern Ireland.

As a result of the outage, a major incident was declared at 09:10 hrs and business continuity arrangements were activated to maintain essential clinical services and to protect patient safety. This involved the following:

- Time critical procedures were maintained and the emergency departments continued to care for existing patients and new attendances.
- An Ambulance divert was put in place away from the two acute hospital sites (Craigavon Area and Daisy Hill Hospitals) with only Category 1 ambulances (excluding major trauma) being accepted by both Emergency Departments.
- To ensure patient safety, most planned surgery and out-patient hospital appointments on 17th September were cancelled and as the impact of the incident evolved a decision was made to also cancel appointments booked for the 18th September.
- Whilst network access was restored by 16:15 hrs on Wednesday 17th September, paper records were retained overnight to ensure safe services were provided to all patients during this period.

In managing the impact of the IT outage, 1,647 patients had appointments cancelled and the Trust worked at pace to rebook all postponed appointments in line with clinical priorities.

The Trust conveys its sincere apologies to all of those impacted by the outage and wishes to assure our patients, service users, and staff that the Trust has prioritised its efforts to ensure that all findings and learnings from the incident are captured for the Trust and are being actively shared with the wider HSC.

4. PURPOSE OF REPORT

The purpose of this Incident Outcome Report is to summarise the work undertaken by the Trust to identify the cause of the IT outage incident, to review the impact of the outage, and to ensure that key learnings and associated recommendations for improvement are captured.

The report commences by providing an overview of the structures established to identify the facts, findings and learnings relating to the IT outage incident, namely the independently chaired IRG, along with its four sub-groups. It proceeds to provide an overview of the scope of work undertaken by the IRG and each of the sub-groups, and summarises their key findings and lessons learned.

The Trust has already commenced work to embed and share the learnings that have been identified – the final sections of this report provide an overview of the learning implementation

work undertaken to date, along with conclusions and recommendations for continued improvement and business continuity resilience, both within the Trust and across the wider health and social care sector in Northern Ireland, moving forward.

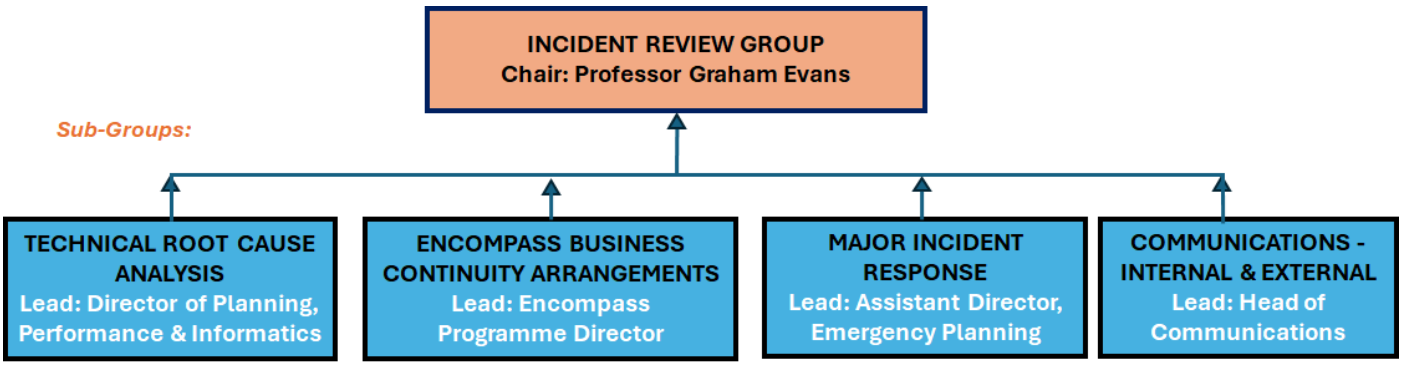
5. INCIDENT REVIEW APPROACH AND SCOPE

5.1. Structure

While a number of working groups were put in place at the time of the IT outage to manage and monitor the immediate technical and business continuity response, the Trust subsequently established a governance structure to undertake a thorough review of the incident and to identify lessons learned.

As outlined in the diagram below, this structure comprised an overarching IRG, which was chaired by an independent industry expert, along with a number of sub-groups.

Figure 5.1 – Overview of Incident Review Group Structure



5.2. Membership

The IRG was independently chaired by Professor Graham Evans, who is a specialist in the area of health and care digital leadership and transformation, having held a number of Executive Director level digital services roles across his 20+ years in the health and care sector in England. Most recently this included being the Executive Chief Digital and Infrastructure Officer (CDIO) and Senior Information Risk Owner (SIRO) for NHS North-East and North Cumbria Integrated Care Board, having recently retired in July 2025.

The other members of the IRG included the Trust's Executive Director of Nursing and the Trust's Medical Director. The identified sub-group leads also attended the meetings of the IRG to provide updates on their respective areas.

The IRG met a total of five times since 14th October 2025.

5.3. Incident Review Group Scope

The role of the IRG was to establish the facts relating to the IT outage incident, including to identify any findings which caused the incident, factors which contributed to these findings,

and to make recommendations which when implemented would serve to reduce the risk and/or impact of a similar incident occurring in the future.

The group also considered the actions taken by the Trust in response to the incident, with a particular focus on learnings and improvements that can be made in respect to the enactment of emergency planning and business continuity arrangements and communications both during and following the incident. A copy of the Terms of Reference of the IRG is included at Appendix 1 of this report.

The Trust is extremely conscious of the regrettable impact on patients and service users during and following the incident. As part of the review work the IRG sought to understand the wider impact of the outage, in terms of the impact on patients.

In completing their scope of work the IRG has been supported by the work of the four sub-groups as outlined in the diagram as section 5.1 above. A high-level summary of the agreed scope of each of the sub-groups is outlined below.

- ***Technical RCA Sub-Group*** **-** to review the Change Control Process associated with the upgrade undertaken to the Trust data centres prior to the IT outage, review the upgrade activity undertaken prior to the IT outage, establish the root cause and analysis, and to propose any recommendations and shared HSC learning.
- ***Major Incident Response Sub-Group*** **-** to review the Trust's major incident response, including general emergency planning and business continuity arrangements. This includes an assessment of the adequacy of the Trust's response and co-ordination arrangements, the effectiveness of business continuity plans, and to identify any improvements for similar incidents in the future.
- ***encompass Business Continuity Arrangements Sub-Group*** - to consider the enactment of the business continuity arrangements in respect to the encompass patient record system in the Trust at the time of the IT outage, with a particular focus on learnings and improvements that can be made in implementing encompass business continuity arrangements going forward.
- ***Communications Sub-Group*** **-** to consider how effectively the key messages were communicated to internal and external stakeholders both during and following the IT outage incident. This includes the adequacy of the communications response in terms of coverage and timeliness to internal and external stakeholders and identification of any improvements in respect to communications for any similar incidents going forward.

A copy of the agreed Terms of Reference for each of the sub-groups is included at Appendix 2, with the exception of the encompass Business Continuity Arrangements Sub-Group which had largely completed their review and learnings work in the days immediately following the incident, which was prior to the formal establishment of the incident review governance structure. The IRG subsequently reviewed the coverage of the scope of work already undertaken by the encompass Business Continuity Arrangements Sub-Group and agreed that this was sufficient to meet the needs of the review.

6. FINDINGS AND LESSONS LEARNED

6.1. Summary of Findings and Lessons Learned

Each of the four sub-groups prepared and submitted Findings Reports to the IRG which summarised the review work undertaken in their respective areas, their key findings, lessons learned, and recommendations for improvement. A copy of the Executive Summary from each of the sub-group reports is presented at Appendix 3 and a summary of the collective findings and lessons learned is outlined in the paragraphs that follow.

Technical RCA Findings and Learnings

Following the successful restoration of network access at 16:15 hrs on 17th September, the Trust's IT team worked closely with the Trust's external network infrastructure support provider and its subcontractor (who provide technical assistance centre (TAC) support to the Trust for all aspects of data centres and wider comms infrastructure) to forensically review system logs, and the timeline of events prior to and subsequent to the incident, with the intention of identifying the technical root cause.

Supported by IT colleagues from across the HSC namely, Western HSC Trust, Northern HSC Trust, the regional BSO, and DHCNI, it was concluded that:

- the change control process associated with the planned upgrades to the Trust's data centres (DC1 and DC2) prior to the IT outage was considered appropriate and proportionate and the correct process and mandate had been followed by the Trust.
- the infrastructure in both data centres was reviewed and is considered to be highly resilient and correctly designed for its purpose.
- the root cause of the outage was as the result of human process error. Review of the detailed technical logs has identified that the outage occurred when a member of the network infrastructure support provider attempted to install the necessary software onto the data centre hardware - the configuration was mistakenly applied to the active data centre (DC1) which was running and not to the inactive data centre (DC2) which was being upgraded.

As a result of the prompt actions of the Trust and its partners, the direct impact of the incident lasted only one business day, which, given its nature could have been far more service impacting. Learning from the incident the Technical RCA sub-group identified a range of measures to mitigate the issue of human process error when carrying out critical upgrades within data centres in the future. The recommendations, which complement the robust practices that are already in place, are summarised in section 7.1 and the Trust has already commenced the implementation of the steps identified to strengthen existing processes.

Business Continuity and Communications Findings and Learnings

This section collectively summarises the findings and learnings from the three remaining sub-groups, namely the Major Incident Response Sub-Group, the encompass Business Continuity Arrangements Sub-Group, and the Communications Sub-Group. Further details are included in the Executive Summaries contained in Appendix 3 to this report.

During the incident, the Trust, supported by its partners, quickly implemented emergency planning and business continuity (EPBC) arrangements in a controlled and coordinated manner. Governance systems and decision support processes all appeared to work with a high degree of effectiveness.

EPBC arrangements were activated promptly, with a 'major incident' declared at 09:10 hrs and the Bronze control structure established accordingly. The incident management response ensured well chaired Bronze meetings with structured decision-making and clear task ownership. Overall feedback was that Trust strategic direction and coordination was effective, with Directors cascading information to their management teams for dissemination, and in parallel appropriate engagement was being maintained with other HSC organisations. However, it was noted that the Bronze meetings would have benefited from defined clinical oversight, time-limited meeting structures, and improved coordination of Sitrep reporting processes to reduce potential duplication. Furthermore, SLT members acknowledged the importance of regular review of the Corporate EPBC plans and the need to periodically refresh training and exercising of major incidents as a group.

Clinical and operational teams demonstrated exceptional collaboration and flexibility, responding to the incident with a calm and patient focussed approach. Many services successfully activated existing business continuity plans, reverting to the use of contingency measures to prevent risks to patient safety. Previously undertaken EPBC training and specific encompass business continuity training proved extremely valuable, with staff who had recently participated in such training responding to the incident more confidently. This was a key learning and has reinforced a need for the identification of EPBC team leads across the organisation, more regular EPBC testing, and robust contingencies which reflect the increased dependency in the Trust on key IT systems such as encompass.

In this regard it is important to acknowledge that the encompass electronic patient record system is relatively new to the Trust having been implemented on 8th May 2025. Trust staff have been outstanding in their efforts to adjust to the new ways of working and workflows that encompass has required and have been successful in achieving a very ambitious encompass stabilisation plan. However, the IT outage incident on 17th September was the first time that Level IV encompass business continuity had been required since go live of the system. Level IV means that staff did not have access to the Trust network which limited access the encompass patient record. Staff were required to utilise alternative Business Continuity Access (BCA) devices within their departments, which requires different ways of working from day-to-day operations or planned encompass downtime. While this was challenging for staff, they managed extremely well under the circumstances to safely care for patients.

The review findings highlighted that there were sufficient BCA devices available and operating as intended. Some staff also utilised additional business continuity facilities to access data from the system, namely Rover devices (being iPhones which contain the encompass 'App') and the Haiku App (which is an App accessible to approximately one third of the Trust's Medical Staff to access medication history, latest observations, allergies, and alerts). This complemented the encompass business continuity procedures and helped ensure that patients had safe continuity of care at the time of the outage. Following the incident, recovery workstreams successfully managed timely back charting of patient records, diagnostics uploading, and appointment rescheduling.

The Trust has gained significant encompass related learning from this IT outage which has been documented and shared with other HSC Trusts and the Regional encompass team. These lessons learned cover a range of areas such as practical advice to teams in terms of suitable access to manual reporting resources, further encompass business continuity training needs, learnings in regard to encompass business continuity governance structures and processes, practical advice regarding back charting processes following an incident, and arrangements to maximise the effective the use of mobile data solutions (i.e. Rover Devices and the Haiku App).

Where applicable the Trust has already implemented actions arising from these learnings, for example, in respect to holding additional encompass business continuity training, ensuring availability of stock to support manual paper processes, adding software to allow for central monitoring of BCA devices, and developing a new standard operating procedure for weekly checks on BCA devices and printing capability. This has already significantly improved the Trust's (and the wider HSC) resilience and efficiency in managing any future similar outages.

In regard to communications, the response to the IT outage was considered to be effective given the challenges of the situation and the lack of access to main internal communication channels, i.e. global email updates. In managing internal operational communications, teams communicated effectively using 'WhatsApp' groups, touchpoint meetings, Teams calls and Trust mobile phones. In terms of corporate communications, regular statements were disseminated using a variety of channels such as social media, internal staff web page, and external media coverage. Long standing relationships with media and elected representatives enabled the Trust to brief these partners who supported and amplified important public messaging, and a dedicated patient helpline was further established from 18th September. Overall, external communications to the public, elected representatives and the media appeared to have been well received, however a number of areas have been identified to improve internal communications with a particular focus on contingency arrangements at times of IT network outages and formal communication mechanisms with regional IT colleagues.

6.2. Review of Digital Governance

As part of the role of the independent chair in providing oversight to the work of the IRG sub-groups, a high-level review was undertaken on the Trust's Digital Governance arrangements. Feedback from the review noted that:

- The Trust appears to have strong leadership and governance with a clear line of sight between the Board and down to ward level.
- The Trust's Vision & Strategy and Annual Plans have strong connections to the Board Assurance Framework (BAF) and associated Corporate and Directorate risk registers, however as further detailed below, it is considered that some areas of this could be strengthened.
- The Trust's technology architecture for the two main hospital sites provides a high level of confidence and assurance.

Observations from the review further identified areas that can be enhanced and strengthened, enabling a more responsive and integrated approach to managing the risk of a range of IT related incidents going forward. These are summarised as follows:

- ***Improved integration of digital data and technology (DDaT) services with operational service delivery*** – While it was noted as positive to see the risk of cyber security threats being recognised at both a BAF and Corporate Risk Register level, a review of the risk details noted that this strategic risk appeared to be 'technically owned' with little reference to 'business ownership'. Similarly, the listed operational and service delivery risk does not currently acknowledge dependency on DDaT services and its critical infrastructure. A major DDaT incident will be an operationally disruptive event, therefore the operational risk needs to reference technology impacts and vice versa.

- ***Risk of critical infrastructure loss/disruption*** – While cyber security threat is a key risk to the organisation, there is also a wider risk associated with the organisation's dependency on DDaT services and critical infrastructure. Consideration should be given to expanding the cyber security risk or adding an additional risk to recognise the risk of loss / disruption of critical infrastructure. Reference should also be added to the application of Business Continuity Plans as a mitigation in the event of a network outage.

- ***Strengthening of Business Continuity Plans to reflect DDaT impact*** – Further to the points above, the Trust is currently considering how to strengthen business ownership of key digital/information assets using Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) to link with operational directorates to co-develop their Business Continuity Plans, ensuring recognition of DDaT service impact on business operations.

The review of the management and ownership of these risks is currently underway, including the review of the digital/information asset ownership within the Trust.

6.3. Impact of the Incident

The Trust is extremely conscious of the impact on patients, service users and staff during and following the incident. As outlined in the findings above, the safety of patients within the Trust's hospitals at the time of the incident was prioritised with business continuity measures activated to ensure that patients had safe continuity of care at the time of the outage.

However, regrettably, most planned surgery and out-patient hospital appointments on 17th September were cancelled and as the impact of the incident evolved a decision was made to also cancel appointments booked for the 18th September. This resulted in the cancellation of a total of 1,647 patient appointments across these two days. The vast majority of these appointments were Outpatient appointments (c.85%), with smaller numbers relating to elective inpatient / day case procedures (c.3%), and the remainder (12%) split across diagnostics, day clinical centre appointments and multi-disciplinary team patient discussions.

Work commenced immediately following the resolution of the incident to ensure that all patients whose appointment was cancelled, and who still required an appointment, were rebooked as quickly as possible. In rebooking appointments, patients were prioritised by clinicians and staff ensuring that highest priority patients were given the earliest available appointments.

The re-booking of all required patient appointments is complete. The last patient appointment re-scheduled for red flag outpatient appointments (new and review) was 5th November 2025 and the last urgent outpatient appointment (new and review) is re-scheduled for 4th February 2026. Furthermore, the last re-scheduled patient appointments for elective inpatient / day case procedures and day clinical centre appointments were 13th October 2025 and 24th November 2025 respectively. The most significant number of appointments requiring re-booking related to routine patient appointments (new and review), with the last routine review outpatient appointment now re-scheduled for 30th July 2026.

No other patients who already held appointments scheduled from 19th September onwards were impacted by these re-booked appointments, i.e. no existing appointments were cancelled to facilitate the re-bookings.

The Trust has undertaken a thorough review of clinical governance systems and complaints data, including the Datix incident reporting system, Care Opinion (being the online platform for patients and service users to share their experiences), and Complaints data to identify any reported adverse impact on patients during the IT outage. This review concluded that there have been no complaints received from patients in respect to the care received during the outage which is a testament to the strong patient focussed clinical and operational response previously noted. Care Opinion data identified a number of positive patient feedback reports, complimenting Trust staff for their calm and professional approach during the IT outage. Furthermore, while there were a small number of minor incidents reported via the Datix incident reporting system there was no significant impact on any patient.

In terms of the financial cost associated with the incident, the Trust has incurred costs for staff overtime to facilitate extended and additional clinics for the timely re-booking of cancelled patient appointments, and to undertake patient record back charting. There has also been an undeniable level of opportunity cost associated with the patient clinical activity lost on the 17th and 18th September and the investment of time by Trust Directors and other staff in managing and responding to the incident and in subsequently facilitating its thorough review. At this time, the Trust is seeking legal advice on the contract and any potential ability to recover the financial costs incurred.

7. CONCLUSIONS AND RECOMMENDATIONS

Overall, the Trust, along with its Health and Social Care (HSC) and technology partners, worked in a responsive manner to minimise the duration of the incident resulting in the full network outage being resolved within one business day. While the Trust demonstrated strong foundations in managing the incident, including established emergency planning and business continuity structures, effective external communications, and committed operational staff, this review has highlighted opportunities to strengthen preparedness, resilience, and internal communications, particularly during Information Technology (IT) system outages. The recommendations contained in each of the sub-group Findings Reports have been consolidated and are outlined below under key themes. Further details can be found in the Executive Summaries included at Appendix 3 of this report.

7.1. Technical

The Technical Root Cause Analysis (RCA) sub-group identified a number of recommendations aimed at reducing the risk of human process error during critical data centre and core network upgrades. Key recommendations include:

1. Ensure “second eyes” are engaged for all work on core network components, i.e. two engineers to be engaged when carrying out future work.
2. Digital capture of all critical infrastructure upgrades to the data centres to be recorded by the Trust to assist with reviews of logs.
3. The Technical Assistance Centre (TAC) to be proactively engaged in advance of any planned or remedial data centre or core infrastructure work – this was not the default position at the time of the incident, however the TAC provider has confirmed a procedure that will facilitate this which the Trust has now enacted.
4. Maintenance windows are agreed, implemented and enforced when carrying out changes to data centre and core network components that affect redundancy.
5. Core data centre upgrades to be submitted to Regional Change Advisory Board for additional governance oversight and awareness.

Overall, these recommendations focus on strengthening assurance, governance, and operational discipline during critical infrastructure works. While developed in response to this incident, they are applicable across other HSC organisations and will complement existing good practice. The above recommendations have already been successfully implemented by the Trust and its technical partners in recent upgrade work.

7.2. Emergency Planning and Business Continuity (EPBC) Leadership, Governance and Preparedness

Effective EPBC arrangements underpin the Trust’s ability to respond to and maintain safe services during disruption. It is acknowledged that the implementation of the encompass patient record system has brought a relatively new aspect to EPBC arrangements within the Trust and it is important to ensure that this continues to be embedded as a core part of wider EPBC planning and preparedness.

The review has highlighted that strong frameworks exist, but Directors must ensure that EPBC planning and preparedness is consistently prioritised, governed and tested at all organisational levels. While several improvements have already been implemented, further actions would enhance consistency, preparedness, and operational readiness. The following specific recommendations have been identified in this regard:

6. Review and update the Corporate Emergency Management Plan ensuring clear coordination structures across tactical, strategic and operational levels, including reference to IT outages and encompass business continuity. Role clarity and responsibilities during incidents should be reinforced, along with regular testing and exercising of EPBC plans (including tabletop and scenario-based exercises) to ensure they remain practical, up to date and effective during prolonged or complex outages.
7. Directors to ensure that all EPBC plans are accessible in hard copy and certify these reflect realistic outage scenarios.
8. Clinical Oversight should be strengthened within the Corporate Emergency Management Plan to support decision making, particularly when considering standing down services.
9. Consideration should be given to mandatory business continuity education and training for relevant staff, including regular encompass Business Continuity Access (BCA) training.

7.3. Communication and Staff Engagement during Major Incidents

Overall, the Trust communications response to the IT outage was considered to be responsive and effective given the challenges of the situation and the lack of access to main internal channels. It is proposed that specific measures are required for internal communications to ensure staff can be reached during system outages. The following is recommended for further consideration:

10. Operational teams to review contingency communication methods as part of their crisis response plans. This should include the maintenance of hard copy plans and contact lists when digital systems are compromised.
11. A dedicated IT and communications outage plan should be developed, to include pre-prepared messages, staff guidance and defined update frequencies.
12. The implementation of a Trust-wide mass notification system to enable rapid, consistent communication with all staff should be considered. Telecommunications should explore text messaging and broadcast alert systems to aid staff communications. In exploring mass communications option, the Trust should consider currently available communication channels, including renewing the Connect Staff Application, temporarily interrupting Trust-wide digital screens to display incident updates and access to Epic 'Message of the Day' functionality (during non-IT major incidents).

7.4. IT Resilience and Digital Infrastructure

The incident reinforced the Trust's reliance on digital systems and the need for greater resilience during IT outages, particularly in light of the Trust's recent implementation of the

encompass system. Strengthening infrastructure, access, and contingency arrangements will support service continuity during both local and regional disruptions. The following is recommended for further consideration:

13. Exploration of options to improve network resilience during core outages, including 4G/5G boosters or independent infrastructure; the activation of SIM cards in Rover devices; the use of 'My Wi-Fi' to enable increased mobile data access during outages.
14. Review of the source and hosting of Trust critical systems, considering the benefits and risks of cloud-based versus on-premises access solutions.
15. Consideration should be given to whether moving to SharePoint online would improve access to Trust communications during system outages.
16. Potential operational access by the Regional encompass team to assist during outages, e.g. to remotely support with patient communications via the system.
17. The establishment of additional backup processes for core services should be considered, such as canteen card payment systems.

7.5. Resource and Operational Preparedness

Adequate resources, flexible planning, and practical contingencies are critical to sustaining services during major incidents. The Trust should ensure plans and equipment are in place to support continuity when digital systems are compromised. The following recommendation is noted:

18. A review should be undertaken of resources and equipment required to maintain service continuity during incidents, with consideration given to requests for additional resources where need is demonstrated.

7.6. Summary

In summary, the Trust demonstrated a strong and effective response to a challenging incident. By addressing the recommendations outlined above the Trust can further strengthen it preparedness and ability to respond more effectively to future major incidents.

8. NEXT STEPS

This report has been shared with the Trust's SLT who will be collectively responsible for assessing the IRG recommendations outlined above and agreeing an action plan to consider their implementation.

GLOSSARY

BAF	Board Assurance Framework
BCA	Business Continuity Access
BCP	Business Continuity Plan
BSO	Business Services Organisation
CAB	Change Advisory Board
Category 1	A situation involving potentially life-threatening injuries and illnesses
CDIO	Chief Digital Infrastructure Officer
DCHNI	Digital Health & Care Northern Ireland
DC1	Data Centre 1
DC2	Data Centre 2
DDaT	Digital Data and Technology
Epic	The Trust's electronic patient record (EPR) software platform
EPBC	Emergency Planning and Business Continuity
EPR	Electronic Patient Record, being the electronic document which has replaced traditional paper patient notes and other legacy applications.
encompass	The Health and Social Care Northern Ireland wide electronic patient record system
HSC	Health and Social Care
IAA	Information Asset Administrator
IAO	Information Asset Owners
IRG	Incident Review Group
IT	Information Technology
JESIP	Joint Emergency Services Interoperability Principles, being a UK-wide initiative to standardize how blue light services work together during major incidents.
LAN	Local Area Network
LIMS	The Trust's Laboratory Information Management System
NIPACS	The Trust's Radiology & Digital Pathology System
RCA	Root Cause Analysis
SHSCT	Southern Health and Social Care Trust
SIRO	Senior Information Risk Owner
SLT	The Trust's Senior Leadership Team, comprising the Trust Chief Executive and Directors
TAC	Technical Assistance Centre

APPENDIX 1 – Incident Review Group Terms of Reference

Southern Health and Social Care Trust
TOGETHER, IMPROVING CARE, TRANSFORMING LIVES

TERMS OF REFERENCE

SHSCT INCIDENT REVIEW GROUP

Name of Group	SHSCT Incident Review Group
Version	Final v1.0
Date	14.10.2025
Context	This Terms of Reference relates to the full network outage experienced by the Southern HSC Trust (SHSCT) at 08:05 hrs on Wednesday 17th September 2025. This outage resulted in a loss of connectivity for SHSCT staff with regional systems including encompass (patient record), NIPACS (radiology & digital pathology system) and LIMS (laboratory information system). These systems remained accessible to all other HSC Trusts in Northern Ireland. Despite every effort, the network infrastructure support provider was unable to resolve the issue quickly, therefore the SHSCT Senior Leadership Team met and agreed next steps as outlined below: • A major incident was declared at 09:15 hrs and business continuity arrangements were put in place to maintain essential clinical services. • Time critical procedures were maintained and the emergency departments continued to care for existing patients and new attendances. • An Ambulance divert was put in place away from the two acute hospital sites (Craigavon Area and Daisy Hill Hospitals) with only Category 1 (excluding major trauma) being accepted by both Emergency Departments. • To ensure patient safety, most planned surgery and out-patient hospital appointments on 17th September were cancelled and subsequently as the impact of the incident evolved the decision was made to cancel appointments booked for the 18th September also. This resulted in the cancellation of 1,632 patient appointments in total. Whilst access was restored by 16:15 hrs on Wednesday 17th September, verified by the network provider by 17:00 hrs, paper records were retained overnight to ensure safe services were provided to all patients during this period. The major incident was stood down at 09:00 hrs on 18th September 2025, however many services remained impacted and continued to follow business continuity arrangements. Manual records had been kept during the outage therefore it was essential to upload this information on to the encompass system to maintain full patient records on encompass and thus protect patient safety. This was completed on 23rd September 2025 for all inpatients across the SHSCT and it is understood that Outpatient recording was later concluded

	by Friday 26th September 2025. The impact on Community services was minimal and all services were fully restored and operational on Friday 19th September 2025. In line with statutory/legislative requirements the SHSCT reported this matter to both the Information Commissioner's Office (ICO) and the Competent Authority (Network Information Systems Regulator).
Purpose	The purpose of this independently chaired Incident Review Group is to establish the facts relating to the IT outage incident within the SHSCT on Wednesday 17th September 2025, including to identify any findings which caused the incident, factors which contributed to these findings, and to make recommendations which when implemented would serve to reduce the risk of a similar incident occurring in the future. The Incident Review Group will also consider the actions taken by the SHSCT in response to the incident, with a particular focus on learnings and improvements that can be made in respect to enactment of business continuity arrangements and communications both during and following the incident.
Chair	The Incident Review Group will be chaired by an independent industry expert, namely Professor Graham Evans. Professor Evans is a specialist in the area of health and care digital leadership and transformation, having held a number Director level digital services roles across his 20+ year in the health and care sector in England. Most recently this included being the Executive Chief Digital and Infrastructure Officer (CDIO) and Senior Information Risk Office (SIRO) for NHS North-East and North Cumbria Integrated Care Board, having recently retired in July 2025.
Membership	**Name** Independent Chair SHSCT Executive Medical Director SHSCT Executive Director of Nursing **In attendance as Project Leads:** SHSCT Director of Planning, Performance & Informatics SHSCT Head of Communications SHSCT Encompass Programme Director SHSCT Emergency Planning Lead Should a member be unavailable to attend, where possible a nominated deputy should attend in their place. Additional Membership: Other colleagues may be invited to join the group as key areas of focus are identified and discussions progress.

Others in Attendance

Title	Role / Responsibility
PA to the SHSCT Director of Planning, Performance & Informatics	Project Admin
SHSCT Senior Head of Planning	Project Support
SHSCT Head of Office	Project Support

Date Established

14.10.25

Scope

The Incident Review Group will be supported by the work of the following sub-groups which have been established to consider various aspects of the IT Outage incident as follows:

Sub-Group	Trust Lead	Anticipated Reporting Date
Major Incident Response, including general emergency planning business continuity arrangements	SHSCT Emergency Planning Lead	14/11/25
Encompass business continuity arrangements	SHSCT Encompass Programme Director	Initial draft prepared
Technical Root Cause Analysis	SHSCT Director of Planning, Performance & Informatics	End October 2025
Communications, internal and external	SHSCT Head of Communications	14/11/25

Each of the above sub-groups shall prepare a Terms of Reference and subsequently a Findings Report in respect to their area of review. It is expected that the Findings Reports shall include the findings of the relevant area of review, along with learnings and recommendations for improvement. Both the Terms of Reference and Findings Reports shall be submitted to the Incident Review Group.

The scope of the Incident Review Group shall include the following:

- Review and approval of the Terms of Reference for each of the sub-groups outlined above;
- Tracking of progress of each of the sub-groups as against the process and timelines set out within their Terms of Reference;
- Provide direction on matters of escalation arising from the sub-groups where required;
- Review and challenge (as applicable) the Findings Report provided by each of the Sub-Groups, ensuring the principles of natural justice are appropriately applied; and

	• Based on the information provided by the Sub-Groups, develop and approve an Incident Outcomes Report that summarises these findings and outlines learnings for the future as detailed in the 'Purpose' section of this Terms of Reference above.
Timeline for completion of the review	It is intended that the review process shall be completed within an 8 week timeframe following the first meeting of the Incident Review Group. This is dependent on the timely submission of the Findings Reports from the sub-groups as outlined above.
Meetings	**Frequency:** Bi-weekly in the first instance. (This can be revised as work progresses with agreement of the group). **Location:** Meetings via MS Teams, unless otherwise determined by the group. **Quorum:** The group will be considered quorate if at least 2 members are present, including the Chair.
Revisions to the Terms of Reference	The Terms of Reference will be reviewed and agreed at the first meeting of the group. Where a need to amend or modify aspects of the agreed Terms of Reference is identified in the course of undertaking the review this will require discussion and agreement by the Incident Review Group.
Reporting	**Meeting Records:** Action notes will be recorded at each meeting and retained. **Incident Outcome Report:** The Incident Outcome Report will be submitted to inform discussion at SHSCT Trust Board and Senior Leadership Team meetings. It is expected that the Incident Outcome Report shall also be required to be shared with senior stakeholders within the Department of Health / Strategic Planning and Performance Group. It is also expected that a summary version of the Incident Outcome Report shall be required to be submitted and presented to the NI Assembly Committee for Health.
Conflict/ Declaration of Interest	Members will be required to declare any interests that may conflict with the group's terms of reference. During a meeting, if a conflict of Interest is established, the member concerned should withdraw from the discussion / meeting and play no part in the relevant discussion or decision. The Conflict of Interest should be recorded in the action notes of the meeting.

APPENDIX 2A – Technical RCA Sub-Group Terms of Reference

Southern Health and Social Care Trust
TOGETHER, IMPROVING CARE, TRANSFORMING LIVES

SHSCT Data Centre Root Cause Analysis (RCA)

Terms of Reference

1. Introduction

This Root Cause Analysis Group has been set up following an IT Outage at the Southern HSC Trust (SHSCT) on 17th September 2025. This group is tasked with assessing the evidence related to the root cause of this event with the aim of understanding how the event occurred and to identify whether there is any learning that could mitigate the risk of a similar even re-occurring. A wider review will be conducted by the SHSCT which will look at the learning in relation to the management of the incident and the enactment of business continuity arrangements during and following the outage. These two reviews will be conducted in parallel and the findings from the RCA will be shared with the Chair of the Incident Review Group.

2. 1. Incident Definition

SHSCT experienced total IT outage on the core network within the Data Centres within the CAH campus site (DC1-Adam, DC2-Eve) on the 17th Sept 2025. Trust IT worked with the Network Infrastructure Support Provider and their subcontractor providing technical support to recover the core network within the 2 x Data Centres. This RCA Group; with representation from SHSCT; HSC Trusts; BSO, DHCNI and the Network Infrastructure Support Provider and their subcontractor will provide analysis of logs and Technical Assistance Centre (TAC) incident details. The RCA Group has been convened to deliver on several key areas: -

- Timeline of Events (2nd Sept – 17th Sept 2025)
- Current Status Assurances
- Review of Core Infrastructure
- Route Cause & Analysis
- Recommendations
- Wider HSC Learning

3. Data Collection

The RCA investigation will be required to gather relevant information and evidence related to the Core Network Outage within the Data Centres. This should include historical data, system logs, incident reports, performance metrics, and any other relevant data sources relating to the incident.

4. Scope and Boundaries

The focus of the investigation should be on the following key elements of the incident that occurred on the 17 September 2025 within the SHSCT Trust and specifically the 2 x Data Centres at the CAH campus.

- A review of the Change control process:
  - The key decision points in the process

CONFIDENTIAL

Southern Health and Social Care Trust
TOGETHER, IMPROVING CARE, TRANSFORMING LIVES

  - The appropriateness of the staff who make decisions on those decision points.
  - The escalation paths where deviation to the standard process occurs.
  - The timeline of the actions; mitigations and impact.
  - Copy of submitted Change Control Request Form.
  - Copy of upgrade plans.

- A review of any related Data Centre activity in the lead up to the outage incidents on 17 September 2025.
- A review of related Vulnerability Management Group logs/ Datix Logs related to Data Centres.
- A review of the 2 x Data Centre configuration at CAH.
- Assurances from the Network Infrastructure Support Provider and its subcontractor that software versions are stable.
- Assurances from the Network Infrastructure Support Provider that Data centres are currently stable, with no inherent risk within the system because of the outage.
- A review of the management of the technical aspects of the incident, including:
  - Was appropriate action taken in time and by the right people?
  - Were decisions made quickly and effectively by staff with the right authority to make them?
  - Were key stakeholders communicated with effectively throughout the process?
  - Were the incident response processes followed?

5. Stakeholders and Participants

Panel Members:

SHSCT Director of Planning, Performance & Informatics – Chair

SHSCT Head of IT - Incident Owner

SHSCT IT Comms Manager - Change Request and Incident

SHSCT IT Business Services Manager - Contract Support

BSO ITS Interim AD - RCA Review

DHCNI Technical Architect - RCA Review

WHSCT Head of Technical Services - RCA Review

NHSCT IT Comms Manager - RCA Review

Network Infrastructure Support Provider Technical Support & Diagnostics - Providing Interim Report & Fault Diagnosis

Network Infrastructure Support Provider Subcontractor (Worldwide Technical Support) - Providing Analysis of Logs and TAC log

SHSCT IT Admin Support

CONFIDENTIAL

Southern Health and Social Care Trust
TOGETHER, IMPROVING CARE, TRANSFORMING LIVES

6. Regularity of Meetings

The RCA initiation meeting was on Friday 19th September 2025. The group will meet on the following dates over the two weeks of the review and will consider extension of the group depending on the ability to draft a final report within these timescales:

Monday 22nd September 2025 16:00 - 17:00hrs

Tuesday 23rd September 2025 16:00 - 17:00hrs

Thursday 25th September 2025 16:00 - 17:00hrs

Monday 29th September 2025 16:00 - 1700hrs

Wednesday 1st October 2025 16:00 – 17:00hrs

Friday 3rd October 2025 16:00 – 17:00hrs

Methodology and Techniques

The investigation should choose an appropriate methodology for RCA such as:

- The "5 Whys,"
- Fishbone diagrams (Ishikawa diagrams),
- **Fault tree analysis**
- Pareto charts.

7. Timeline and Milestones

The RCA should aim to have findings and recommendations within 2 weeks and the report should be presented to the Senior Leadership Team via the Director of Planning Performance & Informatics. However, the timeline for completion of a formal report will depend on preliminary findings from the data centre support team (Network Infrastructure Support Provider and its subcontractor) and will be updated and presented to the Trust Senior Leadership Team following the preliminary findings. This may exceed the two-week initial timeline.

8. Reporting and Actionable Insights

Initial findings of the RCA report should include:

- Interim findings report.
- A process map denoting key decision points.
- A clear description of the root cause(s).
- Evidence supporting the identified cause(s).
- Recommendations.
- Preventive measures to avoid recurrence.

CONFIDENTIAL

APPENDIX 2B – Major Incident Response Sub-Group Terms of Reference

TERMS OF REFERENCE

SHSCT INCIDENT RESPONSE SUB-GROUP

Name of Group	SHSCT Major Incident Response Sub-group
Version	FINAL v0.4
Date	23.10.2025
Context	It has been identified by the SHSCT Incident Review Group that a sub-group is required to review the Trust Major Incident Response, including general emergency planning business continuity arrangements.
Purpose	The purpose of this sub-group is to review the Trust's Major incident response to the IT outage which occurred on 17th September 2025 and provide a Findings Report which will focus on learning and improvements that can be made in respect to the major incident response and general emergency planning business continuity arrangements.
Chair	The Incident Review Group will be chaired by the Trust's Emergency Planning Lead, Assistant Director, Medical Education & Workforce
Membership	**Name** Emergency planning Lead - Assistant Director, Medical Education & Workforce Emergency Planning & Business Continuity Officer Incident Control Room Commander Incident Control Room participant representatives Operational representatives Project Admin
Date Established	October 2025

1

Scope	This sub-group will assess the adequacy of the Trust's Major Incident response and co-ordination arrangements; assess the effectiveness of business continuity plans and identify any improvements for future similar incidents. A review has already been undertaken by the Trust's Medical Director with Senior Leadership Team (SLT) on 2nd October using the Trusts Emergency Planning and Business Continuity Lessons Management Framework. SLT was acting as the Bronze Command Centre, responding to this Major Incident. The outcome of this review is being summarised into the Findings Report. In addition to this, the group will seek commentary via questionnaires from the Senior Leadership Team, Assistant Directors, Heads of Service and other key stakeholders in relation to this major incident response – specifically what the achievements were, what challenges were faced and areas for improvement. This is in line with best practice as recommended by JESIP (Joint Emergency Services Interoperability Principles). Also in line with JESIP, the themes for responses will be as follows: • Communication • Strategic Direction / Command and Control • Co-ordination • Resources • Planning • Training and Exercise. This sub-group will report to the SHSCT Incident Review Group on lessons identified and produce areas of learning for improvement. This will be submitted on the Findings Report.
Timeline for completion of the review	It is anticipated by the Review Group that the review process shall be completed by 14th November 2025. However, this timeline is dependent on co-operation from Directorates ensuring responses to questionnaires are returned within the specified deadlines.
Meetings	**Frequency:** Weekly in the first instance. **Location:** Meetings via MS Teams, unless otherwise determined by the group. **Quorum:** The group will be considered quorate if at least 2 members are present, including the Chair.

Revisions to the Terms of Reference	The Terms of Reference will be reviewed and agreed at the first meeting of the group. Where a need to amend or modify aspects of the agreed Terms of Reference is identified in the course of undertaking the review this will require discussion and agreement by this Incident Review Sub-Group.
Reporting	**Meeting Records:** Action notes will be recorded at each meeting and retained. **Findings Report:** A Findings Report will be submitted to the SHSCT Incident Review Group for review and approval upon completion.
Conflict/ Declaration of Interest	Members will be required to declare any interests that may conflict with the group's terms of reference. During a meeting, if a conflict of Interest is established, the member concerned should withdraw from the discussion / meeting and play no part in the relevant discussion or decision. The Conflict of Interest should be recorded in the action notes of the meeting.

APPENDIX 2C – Communications Sub-Group Terms of Reference

TERMS OF REFERENCE

SHSCT INCIDENT REVIEW - COMMUNICATIONS SUB-GROUP

Name of Group	SHSCT Incident Review - Communications Sub-Group
Version	v0.1
Date	24.10.2025
Context	This Terms of Reference relates to a review of the effectiveness of the Communications response (internal and external) in response to the full IT network outage experienced by the Southern HSC Trust (SHSCT) at 08:05 hrs on Wednesday 17 September 2025. Communications is one of four Incident Review Sub-Groups that will report to the independently chaired SHSCT Incident Review Group which has been established to consider the actions taken by the SHSCT in response to the incident. This subgroup will consider how effectively the following key messages were communicated to both internal and external stakeholders both during and following the incident: - • Time critical procedures were maintained • Emergency departments continued to care for existing patients and new attendances. • An Ambulance divert was in place with only Category 1 (excluding major trauma) being accepted by both Emergency Departments. • Most planned surgery and out-patient hospital appointments on 17 and 18 September were cancelled impacting 1,637 patients. • Measures taken to ensure safe services. • Knock on service impact with explanation of business continuity arrangements. • Service restoration.
Purpose	Review of the effectiveness of the Communications response (internal and external) in response to the IT outage incident and provide a Findings Report which will focus on learnings and improvements that can be made.
Sub-Group lead	SHSCT Head of Communications.
Date Established	October 2025
Scope	Summarise the Trust's Communications approach applied during the IT outage incident and assess the adequacy of this response in terms of coverage and timeliness to internal and external stakeholders. It will also identify any improvements in respect to Communications for future similar incidents.

	Step 1: Initial communications team response The first step will consider how the communications team reacted to the need for an immediate emergency response and how activity was coordinated. **Step 2: Communications strategy and log** Provision of a log of all internal and external communications undertaken identifying the timing, channels, and a summary of the messaging provided. **Step 3: Assessment of Internal Communications** There is some overlap regarding the assessment of Internal Communications with the 'Major Incident Response Sub-Group' which is considering the effectiveness of general emergency planning and business continuity arrangements. As part of this work, feedback has been sought from Senior Leadership within the Trust on several areas including 'Communications'. This feedback will be referenced in the communications sub-group report and will be supplemented by feedback from a further brief staff survey to be distributed via global email, Southern I and Chat with the Chief. Link to survey below. IT Outage Communications survey internal **Step 4: Assessment of External Communications** Some feedback was received at the time from external stakeholders which will be reflected in this report. A survey will also be issued to elected representatives and local media. Link to survey below. **External Survey Link:** **IT Outage Communications survey External** **Step 5: Prepare Findings Report** This sub-group will report to the SHSCT Incident Review Group on lessons identified and produce areas of learning for improvement. This will be submitted via the Findings Report - see 'Reporting' section below.
Timeline for completion	14 November 2025 Subject to stakeholders returning surveys within deadline.
Reporting	**Terms of Reference:** Subject to review and sign off by the Incident Review Group. **Progress Updates:** The Sub-Group Lead will provide updates to the Incident Review Group at fortnightly meetings during October and November 2025. **Findings Report:** A Findings Report will be submitted to the SHSCT Incident Review Group for review and approval upon completion.

APPENDIX 3A – Technical RCA Sub-Group Report Executive Summary

Southern Health and Social Care Trust
TOGETHER, IMPROVING CARE, TRANSFORMING LIVES

TECHNICAL ROOT CAUSE ANALYSIS SUB-GROUP

EXECUTIVE SUMMARY

1. TECHNICAL BACKGROUND

This is a summary of the multi-organisational investigation, conducted by the Technical Root Cause Analysis (RCA) Sub-Group, into the unexpected IT outage at Southern HSC Trust ('the Trust') Data Centres (DC1 Adam & DC2 Eve) on Wednesday 17th September 2025.

The Trust has a contract with an external network infrastructure support provider for the provision of technical support to the Trust IT Comms Team for all aspects of the Data Centres and wider Comms infrastructure. In providing this support, the network infrastructure support provider holds a sub-contract for 24/7 hardware support, replacement of faulty kit, and provision of Technical Assistance Centre (TAC) support.

DC1 and DC2 are designed to give network resilience to IT services and operations within the Trust, working independently of each other during planned upgrades, i.e. should one Data Centre go offline, the other is designed to continue to function and provide IT services with no impact to end users.

2. INCIDENT OVERVIEW AND TIMELINE

A planned Change Request was raised on 26th August 2025 via the Digital Services Change Advisory Board (CAB) to upgrade the Data Centre core infrastructure (Cisco Fusion switches) to the latest software release. The CAB is an internal Trust governance group who review and approve proposed changes to the Trust's technical infrastructure before they are made.

The Change Request to implement identical software updates to both Data Centres was approved by CAB, and the upgrade work was successfully completed on DC1 on 2nd September 2025. Identical works commenced on DC2 on 9th September 2025, however, whilst working to implement the software update a number of challenges were encountered due to underlying hardware faults. The software upgrade was therefore not completed at DC2 and further work was required over the following days to resolve the hardware faults.

This in itself was not the cause of the outage and there was no impact to users while the hardware fixes were being undertaken in DC2. However, when the hardware replacements had been completed and a further attempt was made to redeploy the software on Wednesday 17th September it resulted in a total loss in network access to both Data Centres from 08:05hrs. The Trust IT team worked with the network infrastructure support provider and their subcontractor's TAC support to recover the core network within the two Data Centres, with the network fully reinstated by 16:15hrs.

3. KEY FINDINGS

The Technical RCA Sub-group has concluded several key findings:

- The Change Request submitted to the CAB was for a low-risk software upgrade. Upon review this was considered appropriate and proportionate, and that the correct

CONFIDENTIAL

Southern Health and Social Care Trust
TOGETHER, IMPROVING CARE, TRANSFORMING LIVES

process and mandate had been followed by the Trust.

- The Sub-group reviewed the infrastructure in both Data Centres and concluded that the architecture was highly resilient, designed to work independently, and was correctly designed for its purpose.
- Both the network infrastructure support provider and their sub-contractor reviewed the detailed technical logs and through dialogue and detailed analysis concluded that the root cause of the outage was as the result of human process error. The outage occurred when a member of the network infrastructure support provider, attempted to install the software onto the new hardware (the chassis). The configuration was mistakenly applied to the active DC1 which was running and not to the inactive DC2 which was being upgraded.

4. LEARNINGS AND RECOMMENDATIONS

Learning from the incident the Technical RCA sub-group proposed several recommendations to mitigate the issue of human process error when carrying out critical upgrades within Data Centres in the future:

- Ensure "Second Eyes" are engaged for all implementation and deployment of changes on Core Network components. The network infrastructure support provider and / or its subcontractor to ensure they provide two engineers when carrying out future work.
- Digital Capture (via Teams) of all critical infrastructure upgrades to the Data Centre to be recorded by the Trust to assist with reviews of logs – whilst all actions are recorded in the logs, interaction with graphical user interface is not. This will provide additional data to demonstrate that best practices were followed.
- TAC to be proactively engaged in advance of any planned or remedial Data Centre or Core Infrastructure work – this is not currently the default position.
- Maintenance windows are agreed, implemented and enforced when carrying out changes to Data Centre and Core Network components that affect redundancy. This will ensure default rollback to the point before the upgrade is put on hold to provide a window to remediate any technical issues in real time during the maintenance timeframe.
- Core Data Centre upgrades to be submitted to Regional CAB for additional governance oversight and awareness, as any outage may potentially have a wider HSC wide impact (as was the case in this instance in terms of the operational need to implement ambulance diverts to other HSC Trusts).
- A formal regional reporting mechanism for major HSC IT organisational incidents should be established to ensure effective communication in the event of a similar incident.

To conclude, the recommendations focus on ensuring that human process error is eliminated as far as possible when carrying out critical upgrades to core infrastructure within the Trust Data Centres. These recommendations are equally applicable to other HSC organisations and when implemented would complement the robust practices that are already in place.

CONFIDENTIAL

APPENDIX 3B – encompass Business Continuity Arrangements Sub-Group Report Executive Summary

Southern Health and Social Care Trust
TOGETHER, IMPROVING CARE, TRANSFORMING LIVES

ENCOMPASS BUSINESS CONTINUITY ARRANGEMENTS

EXECUTIVE SUMMARY

1. BACKGROUND TO ENCOMPASS BUSINESS CONTINUITY

encompass Business Continuity was a key workstream during the Trust's implementation planning activities for go-live of the encompass system (the Trust's electronic patient record system) on 8th May 2025. Following go live there continued to be a Business Continuity Stabilisation Workstream and associated workplan in place, led by the Assistant Director with responsibility for Emergency Planning and included representatives from Epic (the supplier of the Trust's encompass system), the Regional encompass team and Trust wide representation. This pre and post go live Business Continuity work ensured the following:

- Availability of Business Continuity Access (BCA) devices and printers to all departments.
- BCA Red folders with clear instructions on how to use BCA devices were provided to each department.
- The instructions printed in the Red Folders are available on the encompass Hub on the Trust's SharePoint (being the Trust's platform for internal communication and document management in respect to the encompass implementation).

There are various levels of encompass business continuity - in the case of the Trust's IT outage incident on 17th September 2025, business continuity was at highest Level IV, as staff did not have access to the internet (Trust network). This was the first time that this level of business continuity was required in the Trust.

In addition to business continuity access devices, the Trust has 2 further levels of business continuity to access data from encompass when there is no network. These are:

- **Rover Devices** - being iPhones which contain the encompass 'App'. Access to Rover devices in community-based settings include SIM cards and allows staff to access encompass whilst they are on the move i.e. outside Trust facilities (e.g. District Nurses caring for patients in their own homes).
- **Haiku App** - approximately one third of the Trust's Medical Staff have access to the Haiku encompass App which can be used by doctors without access to the Trust network to access medication history, latest observations, allergies and alerts.

2. ENCOMPASS BUSINESS CONTINUITY RESPONSE TO THE OUTAGE

The findings in relation to the immediate encompass business continuity response to the outage, as well as the encompass recovery work, are summarised as follows:

Immediate Response – This was the first time that Trust staff were required to implement Level IV business continuity arrangements which requires different ways of working from day-to-day operations or planned encompass downtimes. However, there were sufficient BCA devices available and operating as intended during the outage and the information necessary to safely care for patients was available. The use of Rover Devices and the Haiku app both complemented encompass business continuity procedures in the Trust and helped ensure that patients had safe continuity of care at the time of the outage.

encompass Recovery - Epic provide robust guidance and support on business continuity and recovery and based on these procedures the Trust established a number of workstreams for encompass recovery, including Medicines Reconciliation and Admin Outage & Recovery, Diagnostics Outage & Recovery, and BCA Outage & Recovery.

These sub-groups successfully progressed and monitored encompass recovery work in regard to a range of key activities as follows:

- **Back Charting of patient records** - which concluded on 23rd September for all inpatients across the Trust and by 26th September for all outpatients.
- **Uploading of Diagnostics** – which was completed and fully tested on 18th September.
- **Re-scheduling of Appointments** – with patients prioritised by clinicians and staff ensuring that highest priority patients are being given the earliest available appointments. Rebooking of all urgent and red flag patients was concluded by the end of September.
- **Business Continuity** – this related to the prioritisation of outstanding actions from the Business Continuity Stabilisation workstream. It is important to note that the outstanding post go live actions noted did not contribute to the cause of the IT outage incident, however, as a result of the outage there was rapid action to progress learnings and ensure improvement, including virtual business continuity training and awareness sessions for staff and processes for checking that reports are correct on each BCA device.

3. LESSONS LEARNED

The Trust has gained significant encompass related learning from this IT outage which has already been documented and shared with other Trusts and the Regional encompass team. These lessons learned cover a range of areas such as practical advice to teams in terms of suitable access to manual reporting resources, further encompass business continuity training needs, learnings in regard to encompass business continuity governance structures and processes, practical advice regarding back charting processes following an incident, and arrangements to maximise the effective the use of mobile data solutions (i.e. Rover Devices and the Haiku App).

Where applicable the Trust has already implemented actions arising from these learnings, for example, in respect to holding additional encompass business continuity training, ensuring a small stock of pre-encompass paper stock and pens are available at ward and department reception levels, adding software to allow for central monitoring of BCA devices, and developing a new standard operating procedure for weekly checks on BCA devices and printing capability.

4. RECOMMENDATIONS

It is recommended that further consideration is given to potential future actions arising from the learnings. This includes further BCA training requirements, additional access to diagnostic systems in the event of a regional outage of encompass, activation of SIM cards or My Wi-Fi to enable additional mobile data access, possible operational access for the Regional encompass team to assist during outages (e.g. to remotely assist with the issue of text communications to patients), and to review the source of a number of Trust critical systems (e.g. the merits of cloud versus on premise access).

APPENDIX 3C – Major Incident Response Sub-Group Report Executive Summary

Southern Health and Social Care Trust
TOGETHER, IMPROVING CARE, TRANSFORMING LIVES

MAJOR INCIDENT RESPONSE SUB-GROUP

EXECUTIVE SUMMARY

1. OVERVIEW OF MAJOR INCIDENT RESPONSE

The Trust formally declared the IT outage a 'Major Incident' at 9.10am on Wednesday 17th September in response to the information available on the outage at that time. Emergency Planning and Business Continuity (EPBC) arrangements were then formally activated, with the Bronze control structure established in line with the Trust's Corporate Emergency Management Plan and regular meetings held throughout the duration of the major incident.

2. FEEDBACK ON MAJOR INCIDENT RESPONSE

In assessing the adequacy of the major incident response and effectiveness of the business continuity plans, a debrief structure was established utilising the Trust's EPBC Lessons Management Framework. The debrief involved a session with all members of SLT to work through a detailed debrief questionnaire, followed by the dissemination of a questionnaire through all Directorates. The questionnaire focused on a number of themed areas in line with the Joint Emergency Services Interoperability Principles (JESIP) best practice, with a summary of responses outlined below:

- **Staff Communication:** Operational teams communicated effectively using 'WhatsApp' groups, touchpoint meetings, Teams calls, Trust mobile phones, and community text alerts. However, challenges were encountered by delayed corporate comms, limited notification systems (i.e. unavailability of Trust e-mails), and the clarity of some messaging. The need for earlier, clearer, and more robust alerts for staff was noted.
- **Strategic Direction:** Overall feedback was that Trust strategic direction went well, with Directors maintaining regular communication with their management teams for cascading. The strategic response also ensured appropriate engagement with other HSC organisations. However, it was noted that some staff felt they had limited visibility of strategic decisions and indicated a need for earlier and more consistent communication from SLT, with timelier Bronze meetings facilitated by a more focussed agenda.
- **Command and Control:** SLT praised the incident management response which ensured organised and well chaired Bronze meetings, clear task ownership, and timely decisions. However, it was noted that the initial command structures at the beginning of the incident would have benefitted from better visibility (e.g. being located at the acute site), and wider representation, with clear separation of strategic and operational roles.
- **Co-ordination:** Coordination was considered to be effective overall – SLT noted an excellent response from clinical and operational teams which was calm, well-organised, and patient focused. It was noted that Bronze meetings could be improved with clearer meeting structures, strict timelines and defined clinical oversight. A need was also identified for improved coordination of Sitrep reporting processes to avoid duplication.
- **Resources:** Staff maintained clinical care using a variety of resources, with availability of Trust laptops and mobiles being noted as particularly beneficial. Challenges were noted with Wi-Fi access, the delay in establishing a phone helpline, and identification of a designated loggist for Bronze meetings. It was also noted that clearer expectations need to be in place regarding the potential redirection of staff during such incidents.

1

- **Planning:** Recent EPBC planning work enabled rapid activation of business continuity plans and service interface management, but improvements were suggested in terms of regular EPBC testing, robust contingencies, accessible contact lists, single-point-of-failure mitigation, and identification of EPBC team leads.
- **Training and Exercising:** Staff with EPBC and online encompass business continuity training were more confident in implementing continuity plans, however broader training and regular tabletop exercises are needed to improve awareness of plans, roles, and emergency procedures.

3. CONCLUSIONS AND RECOMMENDATIONS

In summary, the Trust had well established corporate and service-level EPBC plans, which guided the incident response at strategic, tactical and operational levels. However, the review has highlighted the need for up-to-date, robust, and regular testing of plans with clear coordination structures, reinforced staff training and role clarity, and improved strategic communication – especially during IT outages. As such, the following recommendations have been identified to help ensure preparedness for any future incidents:

1. **Leadership & Awareness:** Directors should prioritise business continuity and major incident planning - appoint Directorate leads to liaise with Corporate EPBC and promote preparedness.
2. **Plan Review & Updates:** Review all Business Continuity Plans, updating contact lists, hard copy documents, and contingency arrangements for communication outages.
3. **Plan Flexibility:** Ensure plans allow service continuity during long-term outages with IT support.
4. **Clinical Oversight:** Include a Clinical Oversight Group in the Trust's Corporate Emergency Management Plan for major incidents.
5. **Mass Notification:** Consider implementation of a Trust-wide mass notification system for rapid, standardised incident communication.
6. **Operational Communication:** Use secure messaging (e.g. WhatsApp) for staff coordination during incidents, following information governance guidance.
7. **Training & Exercising:** SLT and staff should undergo major incident training, tabletop exercises. Consider mandatory business continuity education and exercises.
8. **Resource Preparedness:** Support requests for additional resources/equipment to maintain service continuity.
9. **Service Continuity Decisions:** Ensure a measured and careful approach to standing down appointments or clinics to avoid any unnecessary disruption.
10. **IT Incident Protocol:** Update Corporate Emergency Management Plan to include notification to encompass control team for IT outages.
11. **Communication Planning:** Develop IT/Comms outage communication plan with pre-prepared messages, staff guidance, and frequent updates.
12. **Catering Payments:** Establish a backup process for canteen card system payments.
13. **IT Contingency:** Explore options to strengthen network access during core outages (e.g. 4G/5G boosters or independent infrastructure).

APPENDIX 3D – Communications Sub-Group Report Executive Summary

COMMUNICATIONS SUB-GROUP

EXECUTIVE SUMMARY

1. OVERVIEW OF COMMUNICATIONS RESPONSE

This is a summary of the findings from the Communications Sub-Group established to review the effectiveness of the Trust's Communication response, both internal and external, following the unexpected full IT network outage on Wednesday 17th September.

The Communications team immediately activated its emergency response plan following the first Senior Leadership Team (SLT) meeting on the morning of Wednesday 17th September where a major incident was declared. Roles and responsibilities were agreed with communication team members located to cover Trust Headquarters, which was operating as the 'bronze' incident co-ordination centre, and at Craigavon Area Hospital to manage media presence. These team members were supported by others working on site and from home to maximise remote access channels.

Contact was made with HSC partner organisations via two key WhatsApp groups which covers communications staff across all HSC Trusts in Northern Ireland. This enabled colleagues across the region to prepare their own responses given the impact of ambulance diverts from Southern Trust acute hospitals.

The Communications Sub-Group undertook a range of key communication actions which enabled the Trust to deliver strong communications over the outage period. The actions taken forward reflected the fact that the Trust's internal communication methods were limited due to the full outage impacting network access for those on the Trust sites. This restricted the use of typical internal communication methods, such as global e-mail updates, to communicate with Trust staff. As a result, the key communication actions were as follows:

- Regular statements were issued throughout the incident to ensure the public, Trust staff, media, elected representatives, and HSC colleagues were appraised of the situation.
- Regular social media updates were posted on all Trust channels, including the creation of a dedicated section on the Trust website and a dedicated Internal staff webpage to house internal and external communications for staff. This was accessible to those staff who had network access or were working remotely and came back online during the day.
- Responses were provided to media queries with all requests for interviews facilitated.
- All updates were shared with media and local elected representatives, with individual briefings provided on request. This led to some elected representatives helpfully posting updates on their own social channels, signposting the public to the Trust social media channels, and sharing the Trust's position during their own media interviews on the issue.
- The Trust received extensive media coverage for the duration of the incident.
- Public engagement with Trust social media posts was continuously monitored and live feedback provided. This enabled messages to be adjusted and the correction of misinformation in real time, thus minimising speculation or rumour. Notably the Trust acted promptly to refute speculation that the incident was linked to a cyber-attack.

1

- A Patient Helpline was established from 18-20th September for patients whose appointments or surgery was postponed. The helpline received only 78 calls in total, indicating patients received and understood information from other routes.
- Senior Trust representatives attended the live-streamed Assembly Health Committee on 25th September to provide an update to elected representatives.

2. FEEDBACK ON COMMUNICATIONS RESPONSE

To obtain feedback on the effectiveness of communication both during and after the incident, short surveys were issued to staff, media, elected representatives and service users / patient representatives. A total of 400 surveys were completed by Trust staff, who offered many suggestions and ideas for improvement, with the key themes reflected within the 'Recommendations' section below.

Just 10 responses received from the external stakeholders which were mainly positive or neutral suggesting that the media, elected representatives and service users / patient representatives were largely content with the communications approach, which is in line with the anecdotal feedback received at the time of the incident.

3. CONCLUSIONS AND RECOMMENDATIONS

The following key recommendations have been identified through this review:

1. Operational teams to review contingency communication methods as part of their crisis response plans.
2. Telecommunications team to explore text messaging and other broadcast alert options to reach all staff.
3. IT to advise if a move to Sharepoint online would enable access to more Trust communications off the system.
4. Encompass team to consider a request to the regional team for access to the 'Message of the Day' functionality on Epic (the Trust's electronic patient record software platform) during times of service disruption. (**For non-IT related major incidents).*
5. Communications team to explore with the provider of the Trust wide digital screens, whether programming can be temporarily interrupted and replaced with updates during a major incident. (**For non-IT related major incidents).*
6. Communications team to explore feasibility to renew the contract for 'Connect', the staff app which was introduced during the Covid-19 pandemic, and check push notifications.

To conclude, overall, the Trust communications response to the IT outage was considered to be effective given the challenges of the situation and the lack of access to main internal channels. Regular updates were disseminated supporting strategic organisational decisions. Roles and responsibilities were clear and in line with team protocols. In addition, long standing relationships with media and elected representatives enabled the team to brief these partners who supported and amplified important public messaging. External communications appeared to have been well received; however a number of areas have been identified to improve internal communications which will further improve the Trust's ability to manage during such incidents.