Saving lives, Improving lives

NHS
Northern Care Alliance
NHS Foundation Trust

Meeting	**Oldham Health Scrutiny Committee**
Title	**NCA IT Outage Critical Incident Debrief Report**
Author(s)	John Llewelyn, Acting Chief Digital & Information Officer; Allan Cordwell, Head of Group Emergency Planning, Resilience & Response Unit; Nick Gurbanov, Risk Manager, Paul Allison, Planning Accountant
Presenter	David Jago Chief Officer
Date	Tuesday 6th September

We recommend: The Oldham Health Scrutiny Committee is asked to:

1. **Receive the NCA IT Outage Critical Incident Debrief Report including summary of root cause analysis, the safety, business continuity and financial impacts and associated learning to date.**

Part 1: Explanation

Why is this report being presented?	In accordance with the national Civil Contingency Act, formal debriefs and lessons learnt form part of the management of any business continuity and critical incident experience by the organisation. This report summarises the findings from the Digital Critical Incident and lessons learnt; a summary of safety issues and audits of assurance; a breakdown of activity lost and financial impact; costs associated with management of the outage across the NCA; and the lessons learnt from the incident overall management.
Which NCA Ambitions does this support?	Improving quality, safety, experience and outcomes. Improving performance – meeting and exceeding standards.
Where has this paper has been?	This paper is a follow up to the IT Outage Technology and Root Cause Analysis paper presented to Board in June. It includes the summary of responses from the debrief questionnaire completed by key stakeholder teams and financial impact summary to date.
Is consultation required?	N/A
What are the implications for equality, diversity and inclusion?	The activity lost through this critical incident and subsequent business continuity phase of getting back to business-as-usual service delivery will potentially widened inequalities of access that currently exist
What about sustainability?	Throughout the incident management and transition back to business as usual there has been an environmental impact as a result of switching from digital to paper processes.
Freedom of Information	This document is public.
Key Risks	Key risks on this issue are given in Appendix A.

Part 2: Summary

This report summarises the findings from the Digital Critical Incident and lessons learnt. Learning will be used to review existing and new Business Continuity systems implemented or introduced in preparation for any possible Critical incident that may impact the NCA.

Background Summary

On the evening of 17th May the Information Technology (IT) on call team received reports of the Symphony (A&E) system becoming unresponsive. This resulted in calls being logged with EMIS (Symphony support) and Dell and VMware (infrastructure support) and triggered an investigative process. By mid-morning on 18th of May it had become clear that this was an issue related to the Trust's virtual infrastructure which was affecting most clinical systems in the North East Sector (NES) affecting Bury, Rochdale, Oldham and North Manchester (managed by MFT) acute provider teams. An Incident Response Meeting was scheduled and chaired by the NCA Chief Delivery Officer. At this meeting the current risks and impacted areas were identified with the decision made to establish twice daily meetings and for services across the NES and North Manchester to invoke their Business Continuity plans.

Throughout the weekend of the 21st and 22nd of May the suppliers (Dell & VMware) continued to work on the issues with support from the IT & Digital Teams, with Care Organisations maintaining Business Continuity.

On the 23rd of May the decision was made to build an emergency environment to transfer critical clinical services to. Later that day discussions took place regarding escalating to a Critical Incident; and the final decision was made by the NCA Executive in a meeting chaired by the NCA Chief Executive.

Technical analysis concludes that a software defect was the root cause, and the same issue cannot occur again

Since successful restoration of services, the NCA digital team have worked closely with Dell/ VMware technical leads who have been forensically reviewing system logs, the timeline of incident response actions, with the intention of identifying root cause. The output of this work is a formal report from Dell Technologies.

The report concludes that: a software defect in the VMware vSAN software ESXi/vSAN was the root cause and the effects were triggered by a very specific set of conditions which were:

1. The Witness Server (part of the data centre architecture) was disconnected for routine maintenance purposes for a very brief period of time (<5 minutes);
2. "Large objects" were being created as a result of nightly backups running when the witness server disconnected.

It is acknowledged by VMware that disconnection of the witness server would not normally cause any adverse impact, and the creation of large objects during routine operations (including backups) is part of the core design so entirely expected.

On this occasion this combination of events appears to have triggered the software defect which resulted in higher-than-normal network traffic, high latencies, and data unavailability across the virtual cluster.

VMware have subsequently informed us that the software defect was present in version ESXi/vSAN 7.0 Update 1 and update 2 (our previous two versions of their product) but resolved in vSAN 7.0 update 3 (our current version) and subsequent release. **They have stated therefore that the same issue cannot occur again.**

The report further acknowledges that supplier efforts to diagnose and provide workarounds to help restore services as quickly as possible inadvertently impacted the environment to the extent it became irrecoverable. This prompted the decision to evacuate the cluster to save data whilst the root cause work continued.

NCA management of the platform has always conformed with supplier guidance, changes to the environment are strictly controlled by inbuilt product protocols and supported directly by the suppliers and accredited third parties. The set of circumstances that triggered the defect are not abnormal therefore it is concluded that the incident could not have been foreseen.

One further piece of work has been commissioned from NHS Digital (NHSD) to facilitate an incident review with the NCA Digital Trust System Support team (TSSM), considering the Digital team's incident management step by step and reviewing protocols and local policies to identify any further learning or service improvement insight which can help mitigate any future risk and inform the design of the new cluster.

The software defect was not known to the supplier and only discovered through post incident analysis of system logs. The suppliers have now developed public facing documentation highlighting the issue and are sharing with relevant customers.
The suppliers have also committed to do a full architectural review of the NCA infrastructure to understand workloads and optimise performance.

Critical Incident & Business Continuity response was deployed working in partnership with regional and GM colleagues

The NCA has well established Business Continuity (BC) Systems aligned and audited against the ISO 22301:2019 Business Continuity Standard. In the event of a Business Continuity and/or Critical Incident declaration the NCA will establish formal Command and Control arrangements. Silver (tactical) Control Teams were established across the affected sites, they work between the Gold (strategic) and Bronze (operational) levels of command. During the Critical Incident the Gold Command function was provided by the twice daily Incident Response Meetings which were inclusive of GM EPRR colleagues. Sitreps and briefings throughout the incident were provided to system partners, regional and national teams.

Safety of patients was a primary focus of the incident management with controls to reduce harm put in place. Cancellations of treatments, appointments and delays along pathways

Care organisations services; NCA wide services such as diagnostics and pharmacy (D&P); the group patient access and administration (GPAA) service and primary care services were impacted by the IT outage.
Reporting of incidents, including harms, through the Datix system (Datix system remained unaffected by the IT Outage) was able to continue throughout the incident. This provided insight into the reliability of safety systems put in place. NCA governance managers, floor walkers and an NCA governance oversight group for the IT Outage were visible and accessible in the organisation to support staff and maintain patient safety.

of care were a consequence of the outage

Analysis of Datix submissions shows very little change/impact on submission of numbers per day, even with the issue of miscommunication regarding system availability. Where there was a high number of submissions on a particular day this, in the main, related to on the day cancellations in Rochdale theatres where the NCA delivers the majority of High Volume Low Complexity surgeries.

There were 327 incidents of Low harm reported on Datix with the top three areas of risk being Medications related (of which almost half relate to missed drug dosage), documentation and IT security.
Additionally, there were two incidents of Moderate harm (1 Medication error and 1 surgery related incident not reported for 26 days following the incident) and 1 Serious incident reported relating to Bereavement/End of Life in which a referral was made to the coroner containing incorrect patient demographics. Internal investigations are underway for all moderate and above incidents of harm in line with trust incident management policy. 72hr rapid reviews were undertaken to identified immediate actions required and explore potential learning. It is anticipated the current number of incidents reported may increase over the next few weeks or months. For example, there were several missed and delayed doses of the administration of VTE prophylaxis therapy (enoxaparin). Some of these may present themselves as hospital acquired DVT up to three months after the missed/delayed doses.

It is important to understand that further incidences of harm may still be highlighted/detected in the future and will likely be as a consequence of communication failures. Handover of care documents between acute services and primary care were disrupted throughout the incident. Other examples of communication disruption include the shift to handwritten documents and handheld dictaphones as an alternative to inputting data directly into digital patients records. Currently all dictaphone records have not yet been fully reconciled to patient pathways and significant backlogs of scanning documents back into patient records has been created, this will take some weeks to clear. These communication disruptions may require the need for repeat patient attendances and diagnostics and it will be important to consider whether this Critical Incident played a part in delaying treatment and impacting outcomes for those patients. This is particularly relevant to cancer pathways as there is an inability to identify cancer typing amongst the whole G2 list of letters as a consequence of docking digital pocket memos (DPM) on the same date (the cancer access team rely on listening to each dictation to identify the patients priority), this is a learning recommendation for future BC planning.

Ongoing monitoring of incidents and themes will continue via the Care Organisations weekly Safety Summit meetings.

During and post the incident services undertook several assurance audits to test the strength of the business continuity incident safety control measures. The audits and assurance actions included:

- Daily monitoring of referrals received compared with numbers pre – IT outage

- Emergency departments completed casenotes audits to review reliability of delivery relating to onward referrals and plans requiring action; urgent GP letters; other non-urgent follow ups.
- Daily checks on wards to ensure clinical assessments and observations were being undertaken and documented including VTE Risk Assessment, Medications, Falls and Pressure Ulcer Assessment Patient Observation documentation.
- Reconciliation of all paper clinical outcome forms to ensure integrity of patient appointments for follow ups.
- Sites intentionally held onto documents for scanning, for clinical safety reasons and to ensure continuity of care for the patient whilst they remained an in-patient.
- Floor Walkers ensured staff were complying with the business continuity plans and were taking and recording messages from patient calls accurately.
- The Radiology service undertook a retrospective action to ensure all handwritten radiology reports and paper requests generated during the IT outage period have been transcribed into the CRIS system.
- The Radiology service is retrospectively performing a process of reconciling any temporary PAS numbers generated during the period of PAS system downtime with existing PAS numbers, to ensure all images are correctly allocated on the Sectra image system.
- The Pharmacy service is performing a review on the issues arising from the ePMA (Medchart) & Emis Pharmacy Downtime. The report will include an audit of all medication related incidents reported during the IT Outage which were associated with the system downtime.

The incident temporarily impacted the Trust ability to recover planned care with a particular impact on radiology backlogs

During the period of the IT outage, the unavailability of radiology systems; reductions in outpatient clinics and some theatre sessions meant that reporting and treatment capacity was reduced. For radiology this temporarily halted the ability to continue progress in reducing the scanning and reporting backlog reduction programme. Since restoration of the systems, the radiology service has continued the programme of reducing the backlog by increasing capacity (extra substantive sessions, outsourcing to existing providers and further procurement of independent radiology reporting providers). There remains a systems of daily waiting list monitoring, oversight of recovery through the D&P Operations and Performance Committee and Group Risk and Assurance Committee.

Diagnostics and Pharmacy managed their services using BC plans during the IT outage and did not report any significant harm (Moderate, Severe) incidents related to the IT downtime.

Activity loss and the financial impact of the incident cannot be fully quantified but income is not affected due to the block contracts in place.

All A&E activity that took place during the outage will be at base tariff, regardless of what interventions took place. The impact of this cannot be fully assessed until we have back-dated the A&E attendances onto Symphony ED system. A broad assessment could be made from looking at a similar period, assessing the financial value of this and then estimating the value of the same activity is this was all at base tariff.

For hospital admissions depth of coding impact looks to be minimal. Currently there are c100 uncoded spells due to absent clinical documentation. Financial

assessment can only be made when coding is complete (likely to be early August but there will be a cohort of spells that we cannot code). In real-terms, this will not impact our income due to block contracts in place however we need to be mindful of this period when calculating financial values for future contracts, calculation of elective recovery funding or undertaking casemix analysis.

Early analysis indicates circa 1000 appointments/procedures were cancelled with the biggest impact on high volumes specialities such as ophthalmology and rheumatology.

A broad assessment of the cost of managing the incident has been made at this stage but does not include the cost of non-delivery of activity and catching up on backlogs

The cost of managing and recovering from the impact of the outage from a systems and process perspective is currently estimated at £675k with the bulk of the cost across the Digital and Group access and administration teams. Any impact of non-delivery of activity is not factored in at this stage and would require further assessment.

After an incident, thorough de-briefs are carried out to capture issues identified, recommendations to be implemented, and planning assumptions to be reviewed

To enable as many individuals as possible the opportunity to share their experience the NCA de-brief has been completed on Microsoft Forms. To ensure that the de-brief is inclusive the process is anonymous and paper copies were shared with individuals who may not have access to computers by the Governance Teams.
The de-brief covered the NES response to the IT Critical Incident and the impact to our clinical services. North Manchester is part of Manchester University NHS Foundation Trust therefore this report does not cover their response, the de-brief for this locality was completed by their local EPRR Team at their request.
The de-brief covers all areas of the NCA including Community, Acute Clinical Services, Support Services and Corporate functions. The report findings apply to the following:

- Bury Care Organisation
- Corporate Function
- Rochdale Care Organisation
- Royal Oldham Care Organisation
- Diagnostic & Pharmacy
- North Manchester
- Health Economy partners

A total of 285 individuals responded. The NCA De-brief consisted of total of 13 main questions. The de-brief was open from the 24th of June until the 8th of July 2022. Several comments were received and were captured in a word cloud.

The de-brief identified the following findings:

- Bury CO contributed the most with 37% of the feedback followed by Oldham with 30% and then Rochdale with 15%. 3% of the feedback
- provided was from partner agencies which included Primary, GM Gold and Greater Manchester Health and Social Care Partnership.
- The de-brief identified that the majority of NCA services were affected during the critical incident with 69% of returns stating that they were unable to deliver their usual activities. Most activity affected was patient facing.

- Most forms (67%) reported that communication was adequate. Suggestions received on how to improve communication were themed along informing teams earlier of IT issues, clearer communication on what systems (clinical & non-clinical) were affected, better explanation as to what was causing the issue and earlier communication with our partners.
- A breakdown of how the briefings to staff were received shows that:
- 41% via All user emails
- 22% via Word of Mouth (through floor walkers and service leaders)
- 19% via Meetings (Including safety huddles and routine clinical handovers)
- 13% via the Intranet
- 5% via other methods which include WhatsApp and direct emails.
- Only 51% of the forms submitted stated that they looked at their Business Continuity Plans. All services Business Continuity Plans are located on the intranet. Due to the inaccessibility of the intranet services may staff did not have a local copy of their plan. All Care organisations have a hard copy of the plans in their Silver Control rooms for incidents such as IT failure. Comments received in relation to what could be improved include more detail on actions to take in the event of IT failure, and each area needs to have paper copies of clinical systems available to use in the event of IT failure.
- Overwhelmingly 69% of completed de-briefs stated that they felt adequately supported by their leaders and managers during the Critical Incident. In the feedback section the most common word used was support with 11% included in the text.
- 67% of returns felt that patient safety had been compromised during the critical incident. Many of the comments relating to how we can improve patient safety referred to letters and communication shared with primary care etc., potential for patient being lost in the system e.g., appointments, inability to see medical records, access to key telephone numbers, and access to diagnostic results.
- Four of the debrief questions asked for subjective answers in relation to positive impacts, areas of improvement, recommendations, and general feedback. Many of the themes from these comments relate to communications, ongoing IT issues, IT support, record management and patient safety elements such discharge letters and referrals.

The following critical recommendations have been developed using the data captured within the debrief and from responder's personal observations.

The use of all user emails was the most popular method of receiving communications, the development of a process to allow all user emails to be circulated out of hours in the absence of a member of the communications team needs to be agreed.

Explore the use of developing a backup cloud-based system for critical clinical systems such as e-prescribing.

Develop business continuity plan and processes for clinicians to use DPM or an alternative in downtime procedures (absence of G2) that identifies and prioritises cancer and urgent patients.

All reported harm incidents to be continually reviewed and assessment made if any harms occurred due to the Critical Incident. Learning from incidents to be

shared with Care Organisation Governance Groups and corporate teams for on-going improvement actions.

Risk assessments on risk registers to be reviewed and include possible threat of IT failure and contain mitigating actions.

Review from a BC perspective where we have single points of failure in technical/systems workforce expertise within Digital teams and develop recruitment strategy to address

All services to ensure that they have access to appropriate paper copies of electronic documents (documents can either be held locally or in central pool).

All services to review their Business Continuity plans and ensure that there are appropriate details on what to do in the event of IT Failure, including corporate services such as Group access and administration and NCA cancer services.

Emergency Preparedness Resilience & Response (EPRR) to be added to the corporate induction programme to raise awareness and support employees respond to incidents, in particular introduction to the decision-making tools.

All NCA Executives, Directors and Senior Mangers on Call to attend the bi-annual EPRR On Call Training.

Induction training of nursing staff must include orientation and awareness sessions of how paper-based prescription/documentation charts must be used in the event of ePMA/IT downtime.

Appendix A: Risk Assessment

Principal Objective	Principal Risks	CO/GBU Significant Risks	Likelihood	Impact	Key Control Established	Key Gaps in Controls	Controls	Assurance	Gaps in Assurance	Action plan summary	Opening position 2022/23	Q1 2022/23 position	Q2 2022/23 position	Q3 2022/23 position	Q4 2022/23 position	Closing position 22022/23	Target Risk Score
7. Develop our data for improvement, begin to engage widely and deeply across the NCA, starting our journey to improve inequalities.	**Transparent and Timely Data** IF our systems and processes for the reliable, transparent and timely ***capture and*** provision of data are not robust THEN ***our ability to deliver our core clinical services will be disrupted*** and our ability to deliver on the step change in performance improvement, including reducing inequalities, will be constrained. **Risk Lead: Chief Digital and Information Officer** **Executive Digital Health Enterprise Committee (EDHEC)**	**BCO** Effective IT and Digital (12) **RCO** System 1 access (12) Unstable IT (13) **OCO** KPI reporting Delays (12) Children's Reporting (12) **Digital** 1380 Data storage (12) 6755 Cyber Security (12) 6755 Digital Contract Delivery (12) **Corporate** MFT HIVE Implementation (13)	4	5	Business case Developed to bolster Cyber Security Controls with externally provided Security Operations Centre Development of a single Digital Team across both organisations supported by third party expertise where subject matter expertise is hard to secure. Post Transaction plan to integrate Network, data Centre and Hosting solutions Capital Programme to consolidate stabilised infrastructure Enterprise Architecture Function Created to oversee design decisions	Significant Reductions in planned Capital spend will require planned to be delivered across multiple years. Maintaining two PAS systems will allow progress on integration plan but delay final consolidation of IT enterprises. Definitive Root Cause understanding of Data Centre issues not fully resolved Historic data capture Capacity in Analytics/BI team vs demand for data outputs	3	**Departmental Assurance** • Weekly Digital SLT. Monthly joint SLT with ~Informatics and Digital • Technical Design Authority **Corporate Assurance** EDHEC Sub Groups : *Cyber And Information Security Operations sub group* *Enterprise Architecture Board* **Independent Assurance** • Capital Plans and Digital Maturity Trajectory signed off BY GM Digital • Internal Audit review of IT Operational Process • DSP Toolkit submission	Digital & Data Strategy not signed off at Board Recalibrated design and delivery plan for SPR not complete.	• Joint Plan with Allscripts (Altera) to create a simplified Data Catalogue for EPR • Develop new governance and policy to manages consistent data capture in clinical systems • Develop capability within EPR for users to self-report and interrogate data end Q4. • Progress Cyber BC to completion and Procure July 22 (joint procurement with MFT under consideration) • Progress Root Cause Analysis of Major IT Outage to conclusion. June 22 • Take Digital & Data Strategy to Trust Board for approval in July 2022	**12**	**12**					**10**

						Backlog of out of support operating systems to be completed as part of stabilisation Significant Stranded costs and legacy underfunding of revenue position (mitigated by Disaggregation funding) will create cost pressure in 23/24											