NHS Nottingham North and East Clinical Commissioning Group

NHS Nottingham West Clinical Commissioning Group

NHS Rushcliffe Clinical Commissioning Group

Business Continuity Plan Activation and Review

Introduction

This Business Continuity Plan is to be used to assist in the continuity and recovery of the Clinical Commissioning Groups (CCGs) in the event of an unplanned disruption. A disruption could be any event, which threatens personnel, buildings or operational capacity and requires special measures to be taken to restore normal service.

The CCG Business Continuity Plans were activated on Friday 12 May 2017 following the WannaCry Ransomware cyber-attack that threatened local IT infrastructure. This disruption informed a review of the Business Continuity Plan; the plan has been updated and is presented to the Governing Body for approval. The updated Business Continuity Plan has been developed across South Nottinghamshire CCGs based on previous individual CCG plans and learning from this activation.

Business Continuity Plan activation

On the afternoon of 12 May 2017, CCGs' Business Continuity Plans were activated following the identification of infections within the Nottinghamshire IT estate, the network was then taken down to contain and prevent the spread of the infection across the estate. As the incident occurred within working hours, senior managers across the CCGs and the CCG on-call convened to manage the incident and ensure critical functions of the CCGs continued.

The timescales for recovery were unclear and as staff were unable to be relocated or work from home, they were asked to take time owing or annual leave for the remainder of the day. Senior managers continued to provide critical functions over the weekend and an Incident Command Centre was established from Sunday 14 May 2017.

Due to the level of threat to the network, WhatsApp messaging groups were establishsed for local CCG teams and GP practices in response to the incident. Practices were contacted to gain access to buildings over the weekend to support resolution and staff were contacted to ask that they did not switch on mobile devices at home and did not switch on devices when they arrived at work on Monday 15 May 2017. All communication with staffnd practices from the Incident Command Centre over the period of the incident was via the established whatsapp messaging groups.

On Monday 15 May 2017, practices and staff were still unable to access systems and worked offline. From Tuesday 16 May to Monday 22 May 2017 CCG staff were deployed to support recovery of the systems in practices and latterly across the CCG bases. From Tuesday 23 May 2017, most systems across the CCG bases were operational, however, with some access issues and some staff members still involved in supporting recovery of the practices. The Incident Command Centre remained operational until 5.50 pm on Tuesday 23 May 2017 to support resolution of outstanding issues across the practices and CCG bases.

All critical functions identified within the CCGs' Business Continuity Plans were impacted by the disruption.

Rushcliffe CCG) Function	Staff Group e.g. Director/Manager/Officer/Administrator	Number needed	Workstation needed (including: Desk, Phone, PC, access to Printer)	Possibility of working from home on VPN
Leadership	**Chief Officer** **PA Support**	**1** **1**	**2**	**YES** **NO**
Risk management	**Managers**	**2**	**1**	**YES**
Incident Investigations	**Manager**	**1**	**1**	**NO**
Implementation of the Business Continuity Plan	**Manager**	**1**	**1**	**YES**

All critical functions continued throughout the incident, however, for the majority of the incident, operated without workstations and use of mobile phones only. As the incident occurred within working hours, senior managers across the CCGs and the CCG on-call convened to manage the incident and ensure critical functions of the CCGs continued.

The Incident Command Centre was established from Sunday 14 May 2017 to Tuesday 23 May 2017 to deliver CCG critical functions and support the recovery of services to GP practices and CCGs.

All non-critical functions within the CCGs' Business Continuity Plans were also impacted by the disruption.

Service Function	Tolerable Periods of Disruption	
	Minimum	**Maximum**
Financial management including QIPP and financial recovery	10 days	14 days
Planning services - preparing a commissioning plans	28 days	30 days
Commissioning services through pathway development and redesign	28 days	30 days
Performance & data analysis	7 day	21 days
Governance duties to ensure continuous compliance with statutory duties	7 day	21 days
Partnership working to ensure joined up working to improve the health and wellbeing of patients	7 day	21 days
Support and guidance to member practices	2 days	7 day
Administration	2 days	7 days
Clinical Assessment Service	2 days	7 days

Sustainability	28 days	30 days
Integrated working to ensure ongoing delivery of services	7 days	21 days

Support and guidance to member practices was identified throughout the disruption by the Incident Command Centre as a critical function. This was provided throughout the period of disruption, however, communication was initially challenging as there were no previously established methods of communication without IT systems. Support in coordinating the IT functions between commissioned services including acute, community and GP practices was also identified as a critical function for the CCGs during an incident.

Five other non-critical functions, exceeded their minimum tolerable period of disruption, and two non-critical functions exceed their maximum tolerable period of disruption. All other non-critical functions were restored within their minimum tolerable period of disruption.

Financial management was also identified as being required earlier than it's identified minimum tolerable period of disruption of 10 days. This was due to the timing of the incident, finance teams required access to the systems to finalise and submit their annual accounts within required national deadlines. The Incident Command Centre prioritised this function ahead of other non-critical functions.

Summary of results

The activation tested three areas of the plan; activation of the plan as the result of a disruption, raising awareness of a disruption and resolution of the disruption.

1. Activation of the plan

The Business Continuity Plan identified the CCGs' Chief Officers or one of two nominated deputies as needing to authorise activation of the plan. Across the CCGs Chief Officers and Deputy Chief Officers were available and were notified of the disruption on the day and approved activation of the plan at the local bases. The updated Business Continuity Plan is now across the three South Nottinghamshire CCGs reflecting the move towards a shared management structure.

The previous Business Continuity Contingency action plans for loss of established systems for each CCG did not provide guidance or a communincation plan in the loss of all IT across all sites. This has since been reviewed by Business Continuity Leads and updated to reflect the loss of all IT systems across all bases, to include co-ordination of the response and recovery for GP practices, communication plan for practices and establishment of an incident command centre.

The Initial Response Checklist has been completed for the disruption and included as Appendix 1. A loggist recorded all activity within the Incident Command Centre. Records from the Command Centre include the Actions and Responses Log from the Business Continuity Plan.

All critical and non-critical functions were reviewed following the activation of the plan. Minimum and maximum tolerable periods of disruption have been updated for all non-critical functions. The updated business continuity plan also now identifies functions that support continuity of care by commissioned services including acute, community and GP practices i.e. escalation, authorising release of resources as a critical function and notes that finance is impacted differently depending on whether incident is during completion of month end.

2. Raising awareness of disruption

The incident was identified by Nottinghamshire Health Informatics Service (NHIS); systems were then closed down across the network to reduce the spread of the virus. As the incident occurred within office hours, NHIS notified the Director of Outcomes and Information as CCG lead of IT services and staff became aware of disruption as they lost access to systems. Local CCG bases contacted NHIS and were informed about the attack. CCG staff were then notified in person of the reasons for the loss of systems at their local bases. The Business Continuity Plans did not identify a preferred contact for NHIS to notify in an incident. Business Continuity Leads have worked with NHIS to align plan and have agreed a process for notification of disruption to the CCG on-call and individual CCG bases to ensure consistent messages across staff.

The Business Continuity Plans included personal contact details for staff, however, up to date versions were not all available without access to the electronic systems. Whatsapp messaging groups were established for individual CCGs and contact details were provided by line managers and other team members, however, this did mean that not all staff were included in initial communications. The updated Business Continuity Plan details that all documents will be stored securely in paper format as well as electronically.

The Business Continuity Plans included standard contact details for practices, however, due to the loss of systems usual methods of communication were not available. Whatsapp messaging groups were established for practices, however, this took time to establish and did mean that not all practices were included in initial communications. The updated Business Continuity Plan includes mobile phone contact details for all practices.

3. Resolution of the disruption

On identification of the attack, NHIS took down the network to contain and prevent the spread of the infection across the estate. NHIS led the resolution of the disruption with the support of the CCGs' Incident Command Centre. As identified in the Business Continuity Plans, priority was given to provider services.

The incident and responses from NHIS and CCGs has been reported in detail and reviewed separately. Cyber security action plans were developed across NHIS and the CCGs and implementation is monitored by the IGMT Committee. Within the CCG action plan is this review of the CCG internal Business Continuity Plan.

Conclusion

The activation and review highlighted that the CCG Business Continuity Plans required further development to ensure they were effective in the event of all disruptions. The CCG and NHIS responses to the incident have been reviewed and reported throughout the organisations. CCG leads have worked with NHIS to review the learning to ensure that CCG and NHIS Business Continuity Plans are aligned and cyber security action plans have been developed and implementation continues to be monitored. One plan across the South Nottinghamshire CCGs has now been developed that incorporates learning, ensures consistency in approach and reflects the future shared management structures.

The activation was successful in testing the effectiveness of the Business Continuity Plan and identified necessary changes. A further exercise will be conducted within 12 months.

Recommendations

The Governing Body is recommended to:

- **NOTE** the findings of the Business Continuity Plan activation
- **APPROVE** the updated Business Continuity Plan

Appendix 1

Initial Response Checklist

Task	Completed Date/ Time/ By Whom
• Start a log of actions and expenses incurred **(see Appendix 2 of BCP)**	Completed – Hazel Buchanan, Director of Operations 12 May 2017. Continued by Incident Command Centre from Sunday 14 May 2017
• Identify which critical functions have been disrupted	Completed – Local CCG Governance Leads
• Consult with the **Chief Officer of *CCGs*** (or nominated deputy if on annual leave) about activating BCM plan.	Completed - Local CCG Governance Leads
• Advise the **NHS Midlands and East regional team** that this plan has been activated.	Completed – CCG on-call manager
• Seek permission from **the Chief Officers** (or nominated deputy if on annual leave) to suspend non-critical functions.	Completed - Local CCG Governance Leads
Convene CCG Business Continuity Management Team o Evaluate impact of situation o Identify any particularly urgent issues e.g. legal/ contractual timescales etc. o Decide on contingency actions to be taken o Identify staff, resources, equipment etc. required Assign responsibility and timescales	Completed – Hazel Buchanan, Director of Operations 12 May 2017. Continued by Incident Command Centre from Sunday 14 May 2017
• Inform members of the CCG staff (see Appendix 4 of BCP)	Completed – In person at bases
• Inform relevant stakeholders (both internal & external) **(see Appendix 5 contact details)**	Not completed – national media coverage of incident
• Inform Rushcliffe practices if a disruption of core business services is suspected (see Appendix 6 of BCP)	Not completed – Practice systems also affected
• Inform Governing Body members if a disruption of core business services is suspected (see Appendix 7 of BCP)	Not completed – national media coverage of incident
• Access Emergency Pack if required	Completed - Not all required information available

Daily Tasks During the Recovery Process	
• Convene CCG Business Continuity Management Team as necessary to monitor progress made, obstacles encountered and decide on continuing recovery process.	Completed – Incident Command Centre
• Provide updated information to staff & stakeholders	Completed – Staff contacted via WhatsApp messaging group
• Maintain a log of action and expenses. **(see Appendix 2 of BCP)**	Completed – Loggist for Incident Command Centre