

## **Rotherham CCG Business Continuity Policy**

### **Introduction**

The CCG along with its partners has a duty to protect and promote the health of the community, including in times of emergency. We are committed to complying with legislation and guidance in relation to emergency preparedness and business continuity management. Detailed in the '*NHS Commissioning Board Emergency Preparedness Framework 2013*'

The role of the Clinical Commissioning Group (CCG) is to commission healthcare, both directly and indirectly, so that valuable public resources secure the best possible outcomes for patients. In doing so, the CCG will develop, maintain and continually improve the business continuity management systems. This means having suitable plans which set out how the organisation will maintain continuity in its services during a disruption from identified local risks and how the organisation will recover delivery of key services in line with ISO22301. This policy is important because it will help the CCG make sure that it can continue to deliver its business on behalf of patients in times of disruption.

The CCG recognises the potential operational and financial losses associated with a major service interruption, and the importance of maintaining viable recovery strategies.

This policy statement is intended to provide a framework for the CCG to follow in the event of an incident such as fire, flood, bomb or terrorist attack, power and/or communication failure or any other emergency that may impact upon the daily operations of the CCG. It describes the proposed policy for implementing and maintaining a suitable business continuity process within the CCG, including the roles and responsibilities of the officers with the responsibility for implementing it.

This policy statement will support the organisation to think ahead in order to avoid or mitigate risk, take corrective action and be in control of the outcome of an emergency.

The Cabinet Office standard, BS 259999, (now the ISO 22301) lays out the requirements for business continuity management. The business continuity plan (BCP) will be designed to meet the requirements of this standard.

### **Definition - Business Continuity Management (BCM):**

An holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

The diagram (figure 1) illustrates the Business Continuity Management (BCM) Cycle to develop a robust BCM culture across the organisation.



**Fig 1**

### **Aim**

To enable the response to business disruptions to take place in a co-ordinated manner, in order to continue key business operations at the highest level achievable in the circumstances.

### **Objectives:**

- To identify key services which, if interrupted for any reason, would have the greatest impact on the community, the health economy and the organisation.
- To identify and reduce the risks and threats to the continuation of these key services
- To develop plans which enable the organisation to maintain and / or resume key services in the shortest possible time.

### **Scope**

This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

### **What should be included in the Business Continuity Plan?**

- **Business Impact Analysis / Hazard identification – Local Risk Assessment**  
The process of identifying business functions and the effect a business disruption will have on them. Risk assessment is the Process of risk identification, analysis and evaluation using a risk matrix.
- **Critical Activities**  
Those activities whose loss would have the greatest impact in the shortest time and need to be recovered most rapidly.
- **Communications Strategy**  
Internal and external communications and how the CCG cascades information.

### **Examples of where the organisation may need a BCP**

The list below provides examples of what might be considered an event to invoke a BCP. The list is not exhaustive and judgement will be applied in each case:

- loss of workplace short and long term;
- loss of information and communications technology infrastructure services for up to five days;
- loss of key staff short and long term;
- significant national or international incident impacting on the CCG, such as pandemic;
- any requirement as identified by the business impact analysis process;

### **Risk Analysis of the BCP**

The response to an emergency incident does not necessarily or automatically translate into the declaration of a major incident and the implementation of a full recovery operation.

Incidents may cause a temporary or partial interruption of activities with limited or no short term or longer term impact. It will then be the responsibility of the CCG Executive team, as available, to evaluate and declare the appropriate level of response.

The Severity of an incident will be identified as follows:

- Insignificant;
- Minor;
- Moderate;
- Major and
- Catastrophic.

The severity level will indicate the urgency of recovering the business service, and also the order in which services should be reinstated.

The CCG is not responsible for the direct provision of health services, however it is responsible for some functions that have a direct impact on providers of health services, for example safeguarding. Therefore the risks to our stakeholders resulting from a Major incident affecting the CCG could be significant.

A series of robust plans and mitigation will be developed for the following priority incidents:

- unavailability of premises for more than five working days caused by fire, flood or other incidents;
- major electronic attacks or severe disruption to the IT network and systems;
- terrorist attack or threat affecting transport networks or the office locations;
- denial of access to key resources and assets;
- significant numbers of staff prevented from reaching CCG premises, or getting home, due to bad weather or transport issues;
- theft or criminal damage severely compromising the organisation's physical assets;
- significant chemical contamination of the working environment;
- illness/epidemic striking the population and therefore affecting a significant number of staff;
- simultaneous resignation or loss of a number of key staff;

- widespread industrial action;
- significant fraud, sabotage or other malicious acts; and

Immediately upon notification of an incident involving the IT infrastructure, the IT Service Delivery Manager should be made aware of the affected service and obtain an initial assessment.

### **Cascade process**

Immediate response and management functions required to handle an incident will be led by the most Senior CCG Officer on site/on call. A cascade structure will be developed to ensure key individuals within and external to the organisation have been informed.

The CCG Officer will lead any business continuity incident and if necessary utilise the Incident Response Plan to provide any resources required.

### **Accountability**

In order for the CCG to develop a good long-term business continuity capability, it is essential that all staff take on an appropriate level of responsibility.

#### **Governing Body**

BCM is an important part of the organisations risk management arrangements. The Governing Body will ratify this Policy.

Governing Body members need to assure themselves that up to date policies and plans are being implemented effectively in the event of an incident.

#### **Chief Officer / Executive Team**

- Will oversee the implementation of the business continuity policy and standards;
- Will review the business continuity status and the application of the policy and standards in all business undertakings;
- Will enforce compliance through assurance activities; provision of appropriate levels of resource and budget to achieve the required level of business continuity competence;
- Will co-ordinate the overall management of a crisis, providing strategic direction of service recovery plans; and
- ensure information governance standards continue to be applied to data and information during an incident.
- Will decide when to escalate to the area team.
- Will lead the recovery plan after the incident.

#### **Assistant Chief officer**

- Will determine the criteria for implementing the Business Continuity Plan;
- manage training and awareness of the plan; and maintaining the plan.
- will be responsible for change control, maintenance and testing of the plan.
- will ensure the BCP is reviewed and updated at regular intervals to determine whether any changes are required to procedures or responsibilities.

#### **Team managers**

Individual managers will be required to assess their specific area of expertise and plan actions for any necessary recovery phase, setting out procedures and staffing needs and specifying any equipment or technical resource which may be required in the recovery phase.

Individual managers will have two hard copies of the BCP allocated to them. It is intended that one copy should be located at the holder's home address so it is easily accessible and the second in a Folder clearly marked Business Continuity Plan (BCP) at their office base. The BCP folder will also contain recovery procedures, contacts, lists of vital materials or instructions on how to obtain them.

#### **All CCG staff**

- Achieve an adequate level of general awareness regarding business continuity;
- Being aware of the contents of their own business areas disaster recovery plan and any specific role or responsibilities allocated;
- Participate actively in the business continuity programme where required; and ensuring information governance standards continue to be applied to data and information during an incident.

#### **Communications strategy**

Good communication is essential at a time of crisis. A communications strategy should be developed to ensure there are appropriate statements for internal and external communication and processes for ensuring communication to all staff in the case of an emergency. This strategy will be the same across all plans.

#### **Business Continuity and Incident Response Packs**

The Head of corporate Governance will develop business continuity packs to be held in the CCG headquarters.

The contents of these packs will be mirrored, checked for completeness and updated regularly, or whenever there is a change in the BCP which may affect its contents.

#### **Training and awareness**

Once in place, the Head of Corporate Governance will identify appropriate levels of training and awareness sessions for all CCG staff to ensure business continuity becomes part of CCG culture and daily business routines, improving the organisations resilience to the effects of emergencies.

The Head of Corporate Governance will also receive training to ensure they can perform their role effectively and participate in testing.

#### **Testing**

The on-going viability of the business continuity program can only be determined through continual tests and improvements. The Head of Corporate Governance will be responsible for ensuring regular tests and revisions are made to the BCP to ensure they provide the level of assurance required.

If there is a major change to the CCG's role and structure, plans will be tested and revised once a 'settling-in' period has been achieved, to allow for a confident level of response and recovery.

## Business Impact Analysis/Hazard Identification – Local

Hazard	Likelihood	How the hazard affects business	Impact	Risk Score	Controls in Place	Short Term (under 72 hours) action	Longer term action
Fire	1	Loss of use of some or all of premises	4	4	Fire Procedures	Staff work at home or hot desk at other sites where they have access	Temporary alternative work base for key staff, to enable point of contact and email/internet access
Flood	1	Loss of use of some or all of premises	4	4		Staff work at home or hot desk at other sites where they have access	Temporary alternative work base for key staff, to enable point of contact and email/internet access
Terrorist or criminal attack	1	Loss of use of premises. Possible loss of staff	4	4	Emergency response plan	Staff work at home or hot desk at other sites where they have access. Prioritise work if staff affected.	Temporary alternative work base for key staff, to enable point of contact and email/internet access. Prioritise work if staff affected.
Significant chemical contamination	1	Loss of use of premises. Possible loss of staff.	4	4	Emergency response plan	Staff work at home or hot desk at other sites where they have access. Prioritise work if staff affected.	Temporary alternative work base for key staff, to enable point of contact and email/internet access. Prioritise work if staff affected.
IT failure/loss of data	3	No access to email, electronic files, telephones	4	12	IT back-up systems	Remote working through NHSNet. Access to paper files.	As short term
Loss of power	2	No access to email, electronic files, telephones Loss of use of premises	3	6	Back-up generator?	Staff work at home or hot desk at other sites where they have access. Prioritise work if staff affected.	Temporary generator? Temporary alternative work base for key staff, to enable point of contact and email/internet access. Prioritise work if staff affected.
Loss of water	2	Access to Toilets and beverages Cleaning functions	3	6		Staff work at home or hot desk at other sites where they have access. Prioritise work if staff affected	Temporary portable loos Bottled water Water brought in / Stand pipes
Loss of Telephone (landline)	2	Limited telephone communication. Possible impact on email/internet?	3	6		Use of mobile phones. Staff work from home?	Temporary alternative work base for key staff, to enable point of contact and email/internet access
Simultaneous resignation of a number of key staff	2	Loss of leadership function	4	8	Notice period in contracts	n/a	Accelerate normal recruitment processes. Seek secondments to cover gap and provide continuity.
Staff Illness/epidemic	2	Loss of significant number of staff	4	8		Prioritise work.	Prioritise work. Appoint temporary staff where feasible, including secondments from other organisations.

Hazard	Likelihood	How the hazard affects business	Impact	Risk Score	Controls in Place	Short Term (under 72 hours) action	Longer term action
CSU unable to deliver appropriate support	3	Loss of support staff or business functions	4	12	Provisions of the SLA with the CSU	Use directly employed staff and/or agency staff to deliver critical functions CSU action	CSU to remedy. If it cannot, seek alternative sources of support and compensation from CSU.
Travel disruption preventing staff getting to base	3	Loss of significant number of staff	4	12		Staff work at home or at other premises or organisations	As short term, if necessary (long term impact less likely)
Travel disruption preventing staff getting home	3	Staff wellbeing affected. Disruption to work due to need to accommodate staff.	3	9		If possible, obtain food and blankets to enable staff to stay overnight.	As short term, if necessary (long term impact less likely)
Widespread industrial action	2	Loss of significant number of staff	4	8	Staff engagement and HR policies	Prioritise work.	Prioritise work. Appoint temporary staff where feasible, including secondments from other organisations.
Theft or damage to assets	3	Loss of use of e.g. computers, furniture	3	9	Security policies	Staff work at home. Bring old equipment into use?	Purchase or hire replacements
Significant fraud or other criminal act	2	Loss of access to funds? Restriction placed on business activities?	4	8	Security policies	Suspend transactions or seek assistance from partner organisations.	Seek assistance from partner organisations.

Risk Scoring		
No	Probability Scores	Impact Scores
1	Rare	Insignificant
2	Unlikely	Minor
3	Possible	Moderate
4	Likely	Major
5	Almost Certain	Catastrophic

Risk Matrix
Low 1 - 6
Medium 8 - 12
High 15 - 25

#### Notes:

- CCGs will need to develop the detail behind each of the actions in the above, which can be presented as a set of appendices. The actions can be grouped – perhaps as simply as those that affect premises (including IT) and those that are about staff
- All 5 CCGs within SY&B have said that they would support each other with desk space if needed. Premises issues – CCGs will need to discuss with co-occupants of buildings
- IT – to discuss with CSU where it provides IT support to CCGs
- CCGs need to see CSU's business continuity plan, and be assured by it, a part of our business continuity plan

**Business Continuity Matrix (Critical Functions at a glance)**

Department	<b>Priority rating</b> <i>1 = Critical function</i> <i>2 = Can suspend 1-2 days.</i> <i>3 = Can Suspend 3/7 days</i>	Role	ACTION TO MAINTAIN BUSINESS CONTINUITY	
			Immediate	Up to 1 week & Up to 2 weeks
Strategic Planning				
Contracting				
Finance				
Quality				
Medicine Management				
Corporate Business				
Performance				



<b>Management</b>				
<b>CSU functions</b>				
<b>HR</b>				
<b>IT</b>				
<b>CHC</b>				
<b>Communications</b>				
<b>IFR</b>				

# THE

(Insert service Area/Team)

# BUSINESS CONTINUITY PLAN

## WRITING YOUR BUSINESS CONTINUITY PLAN

There can not be one definitive plan as the services that the department offer are very diverse. Consequentially plans will need to be tailored to suit the individual service.

A critical functions analysis has been done so the priorities for each service have been highlighted. Thought now needs to be given to:

- How continuity of highly critical functions can be protected
- How quickly less critical functions can be resumed
- Where possible, through which other means can services temporarily be provided
- Recording the arrangements made that will facilitate the above
- A method to ensure that records are updated

For planning purposes, it may be helpful to think about three separate phases:

**1. The Initial Impact** - What to do if your building is affected whilst in use:

- Evacuation procedures
- What to do with displaced staff
- Who to notify
- Informing Patients

**2. The Immediate Future**

- Notification of telephone contact number
- Temporary arrangements for staff and clients (relocation of the service)
- The giving and explaining of Information to both clients and staff

**3. Longer Term**

- Return to home base
- Resume normal working practices
- Debrief staff to learn from any mistakes made
- Update the plan to reflect lessons learnt
- Periodic test of evacuation procedures and plan

A Plan Template containing specimen forms has been devised to assist in the development of plans. The template should be used as a guide that can be amended to reflect anything specific to the service.

## **Your Business Continuity Plan.**

In addition to completing the basic Business Continuity Planning templates the following information will also need to be included. The 'Initial Questions' and the Analysis questionnaires previously completed will assist you in completing this section of the template.

### ***What to include in the plan:-***

- ♦ **What?** your service does? (Vital tasks - identified by the critical analysis, patient services)
- ♦ **Why?** you do it? (i.e. Statutory duty, public expectation, fee earning, support of other services)
- ♦ **When?** (Target times for getting the service back up and running.)
- ♦ **Who?** (Who are your patients, customers, staff responsible)
- ♦ **Where?** (Locations from which your service is delivered, alternatives available?)
- ♦ **How?** (What you need to provide your service, vital equipment, particular staff, documentation etc)
- ♦ **What?** Existing back-ups in place? i.e. Manual Systems
- ♦ **And** - what would be the consequences to patient care if you could not deliver your service.

### ***Then consider the following:-***

- ♦ Ways to lower the risk - finding alternatives.
- ♦ Ways to protect if alternatives cannot be found, are impractical.

### ***Three stages could be described:-***

- Current situation - the risk to the service as it stands.
- Modified situation - lowered risk by implementing achievable measures.
- Ideal situation - how risk could be minimised if unlimited resources were available.

### ***Scenarios***

You may find it useful to use particular scenarios to demonstrate how you would deal with a particular incident - i.e.

- ♦ loss of access to building (fire, flood, structural)
- ♦ loss of staff (strike, illness, unable to get to work - fuel crisis)
- ♦ loss of communications (phones, computers, software, client information)

Do not forget to refer to existing plans and documents i.e. Building Evacuation Plan which may interlink to your Business Continuity Plan.

A pre-arranged call out/contact system is necessary to ensure that the right people are mobilised to their place of duty and in the minimum time.

## STAFF OUT OF HOURS CONTACT LIST

SERVICE:

LOCATION:

NAME AND ADDRESS	FUNCTION	TELEPHONE	MOBILE

# CRITICAL FUNCTIONS ANALYSIS RESULTS

## DO NOT SUSPEND

SERVICE:

LOCATION:

NAME-	FUNCTION	TELEPHONE	REPORT TO:	TEMPORARY LOCATION

# CRITICAL FUNCTIONS ANALYSIS RESULTS

## SUSPEND FOR 24 /48 HOURS

SERVICE:

LOCATION:

NAME	FUNCTION	TELEPHONE	REPORT TO:	TEMPORARY LOCATION

# CRITICAL FUNCTIONS ANALYSIS RESULTS

**SUSPEND FOR 48 hours to 1 week**

**SERVICE:**

**LOCATION:**

NAME	FUNCTION	TELEPHONE	REPORT TO:	TEMPORARY LOCATION



## ALTERNATIVE ACCOMMODATION ARRANGEMENTS

Where staff are to report until they can return to their regular work base

**SERVICE:**

**LOCATION:**

ALTERNATIVE LOCATION	CONTACT NAME	CONTACT TELEPHONE NUMBER

## CRITICAL EQUIPMENT LIST

**SERVICE:**

**LOCATION:**

[illegible]

## Common hazards associated with working at/from home

HAZARD	EXAMPLE	POSSIBLE OUTCOME
1. DSE Work	<ul style="list-style-type: none"> <li>Poor posture</li> <li>Lack of sufficient breaks away from screen work</li> <li>Poor workstation design</li> </ul>	<ul style="list-style-type: none"> <li>Musculoskeletal Injury</li> <li>Eye strain</li> <li>Fatigue</li> <li>Stress</li> </ul>
2. Manual Handling	<ul style="list-style-type: none"> <li>Carrying items up/down stairs</li> <li>Lifting items of equipment e.g. computer etc. out of a car into a building</li> </ul>	<ul style="list-style-type: none"> <li>Musculoskeletal injury</li> <li>Discomfort in neck, shoulder, or back area due to repetitive work</li> </ul>
3. Slips, Trips & Falls	<ul style="list-style-type: none"> <li>Obstruction of aisles and walkways</li> <li>Poor storage arrangements</li> <li>Insufficient space</li> <li>Trailing leads / cables</li> <li>Uneven or slippery floor (e.g. presence of a step / slope)</li> <li>Torn carpet / hole in floor</li> <li>Poor lighting</li> </ul>	<ul style="list-style-type: none"> <li>No injury</li> <li>Minor injuries e.g. bruise, sprain or cut</li> <li>Major injury e.g. wrist / arm / leg; head injury</li> </ul>
4. Working Environment	<ul style="list-style-type: none"> <li>Poor lighting</li> <li>Inadequate heating / ventilation</li> <li>Noise</li> <li>Space (Lack of sufficient)</li> <li>Distractions – e.g. carer responsibilities, school holidays etc.</li> </ul>	<ul style="list-style-type: none"> <li>Slips, trips &amp; falls; eyestrain</li> <li>Fatigue, dehydration,</li> <li>Headaches; poor concentration</li> <li>Musculoskeletal injury; slips &amp; trips</li> <li>Fatigue</li> </ul>
5. Electricity	<ul style="list-style-type: none"> <li>Insufficient sockets available/ overloaded sockets</li> <li>Damaged leads &amp; plugs</li> <li>Overheating</li> <li>Failure of cord grip at plug</li> <li>Lack of / worn insulation</li> <li>Lack of electrical inspection &amp; testing</li> </ul>	<ul style="list-style-type: none"> <li>Electric shock</li> <li>Fire</li> </ul>
6. Fire	<ul style="list-style-type: none"> <li>Lack of inspection &amp; testing of electrical items of equipment</li> <li>Storage of combustible material e.g. stationery adjacent to radiant heaters etc.</li> </ul>	<ul style="list-style-type: none"> <li>Shock</li> <li>Smoke inhalation</li> <li>Burns</li> <li>Death</li> </ul>
7. Work Equipment (e.g. computer, fax machine, printer etc.)	<ul style="list-style-type: none"> <li>Heavy, unwieldy equipment</li> <li>Old or poorly maintained equipment</li> <li>Lack of user training</li> </ul>	<ul style="list-style-type: none"> <li>Musculoskeletal injury</li> <li>Faulty equipment - possible electric shock</li> </ul>

## Business Continuity Plan - Communications

### Introduction

During a period of business continuity it is vital that communication is managed effectively with a variety of stakeholders. This plan supports this management before, during and after any incident that is detailed within the business continuity plan.

For a CCG specific incident the business continuity and communications leads will work together to ensure clear and consistent communications activity. The main aims will be to:

- Deliver relevant messages about the incident to the relevant stakeholder group/s
- Utilise media channels (radio and print) to reassure and inform the public and patients
- Ensure that messages are timely and relevant to the target audience.

### Stakeholders

Our stakeholders are divided into two categories – internal and external – with specific communications mechanisms for each one.

**Internal** - Staff – Oak House based, Strategic Clinical Executive members – GP leads and Governing Body members

**External** - GP Practices, Media, Local Authority, NHS England Area Team, RDASH colleagues, The Rotherham Hospital Foundation Trust, Healthwatch and Voluntary Action Rotherham

### Methods of Communication during an incident

The communication activity used will be activated in conjunction with any incident detailed in the business continuity plan and will be specific to each of the relevant stakeholder affected.

#### Internal Stakeholders

##### Staff, Governing Body members and GP leads

It is essential that we inform staff and keep them up-to-date with any incident that impacts on the ability to undertake their role or has a direct impact on the organisation. This incident could be triggered by a multi-agency source or from within the CCG. The methods used to communicate with staff will be:

- Text message/phone call – used to disseminate an initial message about the incident, containing immediate actions needed and how further messages will be communicated. This is most useful when the incident occurs out of office hours.
- Email – Staff can receive messages via the CCG's distribution lists (held electronically) in normal working hours
- Intranet – Information to be posted on the CCG's home page before and after the incident. Any information during an incident should be communicated through other mechanisms as access may be limited.

- Website – Staff Watch information where staff can get up-to-date information without having access to CCG specific systems. This section of the public site could be updated remotely and would ensure that everyone could access accurate, timely information.

## **External Stakeholders**

### GP Practices

Member practices of the CCG would be informed of any incidents relating to business continuity via email. Contact details for the CCG throughout the affected period would be shared and practice staff would be advised to visit the CCG website for updates.

### Media – print and broadcast

Managing the media should take place in line with the CCG's Media Handling protocol. The communications team have good links with the media, which would be utilised for any incident that requires information communicating to local people and patients. Local radio stations would be able to broadcast public information in their regular bulletins. Information would be issued to the local printed media dependent on the incident timing in relation to the paper publication day. Media statement may be required following an incident and once normal business has resumed. Information would also be published using the CCG's social media sites with links to the website for more detail.

### Partners – Local Authority, NHS England Area Team, Voluntary Sector and Healthwatch, CSU

When an incident impacts on the business of the CCG it is imperative that we inform colleagues at our local partner organisations. Depending on the nature of the incident this would be done either by telephone or by email – via the Chief Officer, Chair or Business Continuity lead. Partner organisations would be encouraged to disseminate the details to their staff via communication channels.

### Providers – All providers from who we commission a healthcare service

Depending on the nature of the incident this would be done either by telephone or by email – via the Chief Officer, Chair or Business Continuity lead. Provider organisations would be encouraged to disseminate the details to their staff via communication channels, providing details of alternative ways to contact the CCG during the period of the incident. Notice would then be given once the incident was resolved and normal business resumed.

Key contacts within the CCG should advise counterparts in the provider organisations of their contact details during the incident.

## **Out-of-Hours communication**

There is no formal out-of-hours communication service within the CCG, however senior officers have been provided with the Communication Manager's mobile number should be contacted in the case of an incident that may affect business continuity. Messages and notifications can be posted on the public website using an internet connection in any location and there are a number of officers with the organisation who access to the admin section.