Business Continuity Plan – Data Security

This document contains suggestions for how you can develop your Business Continuity Plan in terms of data security. Due to the diverse nature of the sector it is not possible to cover every possible scenario. You should take time to judge what possibilities might impact your organisation and to develop a continuity plan to implement in each given scenario.

Data security plans should be added to your existing Business Continuity Plan. This document only covers electronic data as we presume that your existing Business Continuity Plan will cover risks to paper-based records; e.g. fire, flood, loss of records etc.

The Care Provider Alliance has produced guidance on contingency planning.

1. What critical systems do you have?

As a first step you should consider which systems you have and how business critical they are. This will help you to prioritise your Continuity Plan.

You need to know which systems are essential for you to keep providing services. In the instance that you are using electronic care planning software then this is likely to be the most critical system for you.

Common digital systems in the care sector are:

1. Care planning software
2. Electronic Medication Administration Records (eMARs) / Medicine Management
3. Rostering Systems
4. Payroll Systems

If you use any of these then you should prioritise them.

There is a checklist to work through on the next page. This tells you how to create your business continuity plan. If you require further guidance NHS Digital have written a good practice guide.

2. Business continuity plan checklist

Checklist	Date Completed
Identify critical systems	
Identify key suppliers i.e. rota software, IT support, care planning software, Broadband supplier etc.	
See if your suppliers have their own business continuity plans	
Ensure you have contact details for all suppliers	
Ensure all digital hardware i.e. computers, mobiles etc, are recorded	

Scenarios to Consider – think about the following scenarios and write down how you would resolve the situation and how you would operate to maintain essential services until the situation resolves. In many instances this might mean reverting to paper.
What would you do if the phone line or broadband went down?
What would happen if you had an IT system failure?
What would you do if you were hacked?
What would you do if there was a power outage?
What would happen if your supplier had a fault? i.e. your rota system won't work and it's the supplier's fault?

Once you have considered these scenarios	Date Completed
Ensure staff are aware of plans	
Update policies and procedures to match your continuity plan	
Ensure all staff are aware of the plan and what to do	
Ensure there are back-ups of system critical information and your network	
Test the Business Continuity Plan at least annually	