**FAQ: Making the most of digital for your care business webinar with** [**RSM UK**](https://www.rsmuk.com/what-we-offer/industries/healthcare)

* Why should I invest in digital transformation now?  
    
  **Technology is moving so quickly, it’s critical to have foundations in place now to support your strategic growth plans. Modern systems will reduce the risk of cyber-attack and will help you use your staff more efficiently and provide better care. Also, staff retention, if you have good systems that are easy to use, you are more likely to hold on to your staff. If there is a data leak, this can quickly damage your reputation in the market and your relationship with the NHS and local authorities. In line with GDPR, an organisation needs to demonstrate a reasonable level of control of their data, e.g. controlling access to data and data encryption. With the range of tools and technology available today, you don’t have to invest huge amounts of money, to see results, e.g. start with a small use case where you can get some quick wins.**
* What is the return on investment? How long may that take?  
    
  **Smaller targeted investments could return very quickly, e.g. automating small processes, but larger transformations, e.g. full finance/care system replacement programmes, typically return in cash terms over a 3-5 year period, along with other intangible benefits, such as increased brand value and improved working conditions for staff.**
* I wondered if the panel could comment on how effective they consider cyber security insurance is and how important this is to a robust response plan? Obviously, there are lots of policies out there, but just their general impression of its fitness for purpose where clients have got cover.

**The cyber insurance market is evolving rapidly with a wide range of new insurers and products. It’s fundamental to undertake a risk assessment and analyse your cyber risks and key controls in your organisation which can determine your cyber insurance package and level of protection.**  
  
What do you need to be aware of when selecting cyber insurance? Do you need a robust strategy in place?

**Typically, key controls areas insurers are looking for include coverage of all your systems, the level of controls and staff access, keeping staff updated on cyber training and keeping your systems updated with the latest security updates.**

* How do I know if my data has been breached?  
    
  **There is a new level of sophistication of data breaches now, where hackers can delete their audit trail. It’s key to have good quality detection and monitoring systems in place on a multi-layered basis, which create alerts when there’s been a breach, or a breach could occur.**
* The panel has focused mainly on internal considerations.  What are their recommendations in relation to managing digital risk (AI risks, data compliance, security) in the supply chain?    
    
  **The more third parties in your supply chain, the greater your risk exposure. There has led to increased third-party assurance reporting, such as ISE or AF reports, internal audits of third parties. As part of your third-party take-on process, it’s important to undertake a risk assessment of the third-party and due diligence to evaluate whether they have robust levels of control in place. This can form part of your service agreements/contracts. With an increase in cloud-hosted applications, as part of your due diligence, it is important to ask where your third-party data is stored and how secure that data is.**
* In a smaller organisation, the absence of an information officer, where should that responsibility sit?

**It is important to have a reasonable level of control in place. For a smaller care organisation, this could be at an operational level. With confidential personal data, the individual needs know where that data resides and have a reasonable level of control in place to protect the data, e.g. locking filing cabinet/password protection of computer files. In the event of a data breach, this can help avoid fines, as you have demonstrated reasonable care to protect data.**

* With so many sources of data, how can organisations and leaders ensure trust in the data they’re provided for decision making?

**It is important to question everything that is put in front of you; where has the data come from, what systems has it passed through, who has manipulated the data, is it the most current? This can determine the level of confidence in the data and how valuable it is for making decisions.**

* How should we ensure that the right practices are in place around AI for care providers, government, the regulator and organisations like RSM?  
    
  **AI regulations are likely to be developed at an industry-specific level. The key issue will be explainability and transparency - whatever you use AI for, you must be able to articulate what data has been used in the model to drive the outcome and why. If you can’t demonstrate this, you should not be using AI. There will be certain use cases that will be deemed high risk and will require closer scrutiny and some use cases will be prohibited. The CQC is likely to get more involved over time with AI regulations. We are a long way from machines making decisions without human input, ultimately the person making the decision must be comfortable that it’s the right thing to do.**
* How RSM can assist businesses in this area?  
    
  **RSM UK has a range of technical and industry specialists that can support your business with a broad range of digital, data and cyber challenges. We are happy to have a complimentary initial conversation with you to understand what support you need, so please do get in touch with any of our specialists who presented today.**