Client Briefing August 2022

Cyber Security – Matters Beyond our control?

BACKGROUND

It was recently reported in the national media that NHS 111 was subject to a cyber-attack (ransomware based) which caused a 'significant outage' at the service. The reports noted that a malicious attack on the software systems of an external supplier (Advanced) who provide digital services to the NHS had caused the outage. The outage was reported to have affected several key systems used by NHS 111 - including those related to patient referrals and ambulance dispatch. It was reported that contingency plans at NHS 111 had been enacted.

The company involved provide a range of services to NHS organisations. It further transpired that several other systems provided to NHS organisations were also affected by the outage. It has been reported that it will take several weeks for some services to be restored and full details are provided on the Advanced Company website:

https://www.oneadvanced.com/cyber-incident/

The systems reported by Advanced as being affected ('directly or indirectly') are as follows:

Adastra – emergency care clinical patient management system,
Caresys – care home management system,
Odyssey – primary care clinical decision support tool,
Carenotes – community and mental health care note management system,
Crosscare – clinical management system for hospices and private practices,
Staffplan – staff scheduling system,
eFinancials – financial management system.

COMMENTARY

The event perhaps serves as a 'wake-up call' for all NHS organisations in respect of their cyber security arrangements – particularly those that might impact on services and systems we rely on that we procure from business partners and suppliers. The cyber security arrangements (and business continuity arrangements) at these partner organisations could perhaps be seen as 'beyond our control.' However, the reality is that the NHS can do a great deal to influence the design and application of cyber defence and business continuity controls in place in partner and supplier organisations.

Some of the key questions are about how NHS organisations actively manage supplier contracts to reduce the risks associated with cyber attacks against supplier organisations. As a very minimum NHS organisations need to establish whether their key suppliers are applying the same disciplined approach to cyber security as we do at NHS organisations.

In particular – NHS organisations should consider the following key questions in respect of all suppliers:

A checklist of key immediate considerations for NHS Organisations

Immediate Key Considerations
Have we a documented systematic process in place to identify key suppliers and to assess cyber and business continuity risks associated with those suppliers?
Are our contracting arrangements and controls sufficient to actively enforce the basic controls set out in standard NHS Terms and Conditions for supplies? (See Below)
Do our key suppliers have sufficient preventative controls to minimise the risk that they will be subject to cyber-attack?
For each of our suppliers – do they have sufficient strategies in place to mitigate the impact of cyber-attacks should they occur?
Do each of our suppliers have sufficient business continuity arrangements in place to reduce the impact of any cyber-attacks they encounter?
Do each of our suppliers have sufficient business continuity arrangements in place to restore any services 'lost' because of cyber-attacks quickly and effectively?
Are all our supplier contracts sufficiently clear in respect of each party's responsibilities in respect of cyber security and business continuity?
Do we actively check that suppliers have appropriate arrangements for continually assessing and testing business continuity risk? Do we request and receive appropriate evidence from them? Is this being done both before contracts start and regularly throughout the course of contracts?
Do we build into contracts a requirement for suppliers to provide alternative arrangements in the event of a cyber-attack that disables the primary system/service being provided?
If not – is the requirement to cover off the potential service gap resulting from an outage covered in our own internal Business Continuity Plans?
Do we insist that all key suppliers complete a Data Security and Protection Toolkit assessment, or equivalent? • Have all key suppliers achieved a sufficient level of performance against all requirements in the DSPT?
Have any/all incidents of data loss or breach of confidence been recorded, reviewed and reported in accordance with Department of Health guidelines?
Have we (the NHS) specific nominated an information governance lead with clearly defined responsibility to liaise with each key supplier?
Do our policies (the NHS) fully describe individual responsibilities for handling Personal Data and including those involving Suppliers? • Do we actively check to make sure we are applying all policies vigorously and effectively?

We would recommend that for each of the questions above organisations consider how they are assured – i.e., what active steps are being taken to provide real time assurance that supplier cyber risk controls and business continuity arrangements are adequate.

KEY RESOURCES

DATA SECURITY AND PROTECTION TOOLKIT

In considering the questions in the Initial Checklist above we would recommend that organisations consider the stipulations laid down in NHS Digital's Data Security and Protection Toolkit (DSPT) and consider the simple question – **have our key suppliers considered the same self-assessment assertions – and if so – are we confident that their arrangements are sound?**

Section 10 of the 22/23 Toolkit includes several assertions related to 'supplier management and assurance'. See Appendix 1 below for further details.

It is recommended that all NHS organisations recheck their current statuses against each of the stipulations listed in the toolkit.

It should be noted that the toolkit specifies that all suppliers who have access to personal confidential information should complete a Data Security and Protection Toolkit assessment. This is also specified in the NHS Standard Conditions for Supplies (see below). The toolkit provides a basis for assessing the strength of an organisation's arrangements across a range of key data security areas. **The key question is therefore whether our contracting arrangements are actively enforcing this requirement? And are our arrangements ensuring:**

- **That suppliers are completing assessments with appropriate vigour**
- **That suppliers are completing assessments on a regular and timely basis**
- **That action is being taken in respect of any deficiencies noted in those assessments**

NHS STANDARD CONDITIONS FOR SUPPLY

The principles above are also captured in the NHS Standard Conditions for the supply of goods and provision of services. Key extracts relating to supplier business continuity and supplier information and data security can be found in Appendix 2 below. The principles are also well described in the **Information Commissioner's Office (ICO) Contracts Checklist Guidance** which is summarised in Appendix 3 below.

EPRR CORE STANDARD 55

In addition, NHS organisations need to be guided by the content of EPRR Core Standard 55 which outlines requirements around supplier business continuity.

Business Continuity	**Assurance of commissioned providers / suppliers BCPs**	The organisation has in place a system to assess the business continuity plans of commissioned providers or suppliers; and are assured that these providers business continuity arrangements work with their own.

Example of Good Practice

One NHS organisation we serve has built supplier business continuity into its draft Procurement Risk Assessment and Risk Register policy. The procedure sets out a process for the management of risk within the organisation's supply chain in respect of contracts of supply and key suppliers. It starts from the premise that all risk cannot be eliminated – but that it is vital to have a process which helps the organisation identify and understand what its key risks are and a process for managing those risks. The approach in the draft policy will ensure that there is risk assessment built in at every contract stage – meaning that risk is managed and minimised before contracts start and through the whole life of each contract.

As a first step organisations may wish to consider whether they have documented a systematic approach to identifying and managing supplier associated risk. A policy document is a good first step in defining requirements and expectations with regards to managing supplier cyber security and business continuity risks.

CONCLUSION

NHS Organisations may feel that cyber security risks at partner and supplier organisations are 'beyond our control.' However, NHS organisations have many tools in their armour to reduce their exposure to these risks.

The checklist above, together with careful reference to the key resources above, will help organisations to assess the likely strength of their own arrangements and will help organisations to address any significant gaps in those arrangements.

Audit Yorkshire is happy to support our clients in reviewing your systems and processes. Please contact your Internal Audit Manager if we can support you in any way.

August 2022

APPENDIX 1

Data Security and Protection Toolkit 2022/2023 Key 'Supplier Oversight' Clauses

Assertion	No.	Evidence Text	Tool Tips
The organisation can name its suppliers, the products and services they deliver and the contract durations	**10.1.1**	The organisation has an up-to-date list of its suppliers, which enables it to identify suppliers that could potentially pose a data security or data protection risk to the organisation. The list includes which suppliers process personal data or provide IT services on which critical services rely, details on the product and services they deliver, contact details and contract duration.	Provide a list containing suppliers that handle personal information, systems/services and contract start and end dates. The list must have been reviewed since 1 July 2022
	10.1.2	Contracts with all third parties that handle personal information are compliant with ICO guidance.	A review of all contracts has been undertaken to ensure that they comply with the requirements set out in Article 28 of the GDPR. If you have no such suppliers, then 'tick' and write "Not applicable" in the comments box.
Basic due diligence has been undertaken against each supplier that handles personal information	**10.2.1**	Your organisation ensures that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.	This enables the organisation to confirm that the supplier has the appropriate information security accreditations/certifications, prior to signing the contract. The NHS Improvement 2017/18 Data Security Protection Requirements: guidance states that these could include; ISO 27001:2013, Cyber Essentials, Cyber Essentials Plus, or meets the Digital Marketplace requirements. For more information see the [2017/18 Data Security Protection Requirements guidance](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/675420/17-18_statement_of_requirements_Branded_template_final_22_11_18-1.pdf).
	10.2.2	Contracts with all third parties that handle personal information are compliant with ICO guidance. A review of all contracts has been undertaken to ensure that they comply with the requirements set out in Article 28 of the GDPR.	If you have no such suppliers, then 'tick' and write "Not applicable" in the comments box."
	10.2.3	Percentage of suppliers with data security contract clauses in place.	The percentage snapshot of current suppliers handling personal data that currently have security clauses. The organisation may need to update its supplier model contract to include data security and protection clauses/requirements.
	10.2.4	Where services are outsourced (for example by use of cloud infrastructure or services), the organisation understands and accurately records which security related responsibilities remain with the organisation and which are the supplier's responsibility.	The organisation formally documents the roles and responsibilities of both parties to achieve clarity as regards accountability for data security and data protection risks.
	10.2.5	All suppliers that process or have access to health or care personal confidential information have completed a Data Security and Protection Toolkit, or equivalent.	Provide confirmation that all suppliers have successfully completed a Data Security and Protection Toolkit or the organisation has assured itself separately that they reach a similar or higher data security standard.

All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented	**10.3.1**	List of data security incidents – past or present – with current suppliers who handle personal information.	All current ongoing incidents are listed and all historical incidents (up to 2 calendar rolling years). Redact any sensitive information.

The full toolkit is available at:

https://www.dsptoolkit.nhs.uk/StaticContent/Attachment/660

APPENDIX 2

KEY EXTRACTS FROM NHS TERMS AND CONDITIONS FOR THE SUPPLY OF GOODS AND THE PROVISION OF SERVICES (CONTRACT VERSION – GENERAL TERMS AND CONDITIONS)

BUSINESS CONTINUITY PROVISIONS

6 Business continuity

6.1 The Supplier shall use reasonable endeavours to ensure its Business Continuity Plan operates effectively alongside the Authority's business continuity plan where relevant to the supply of the Goods and the provision of the Services. The Supplier shall also ensure that its Business Continuity Plan complies on an ongoing basis with any specific business continuity requirements, as may be set out in the Specification and Tender Response Document.

6.2 Throughout the Term, the Supplier will ensure its Business Continuity Plan provides for continuity during a Business Continuity Event. The Supplier confirms and agrees such Business Continuity Plan details and will continue to detail robust arrangements that are reasonable and proportionate to:

6.2.1 the criticality of this Contract to the Authority; and

6.2.2 the size and scope of the Supplier's business operations,

regarding continuity of the supply of the Goods and the provision of the Services during and following a Business Continuity Event.

6.3 The Supplier shall test its Business Continuity Plan at reasonable intervals, and in any event no less than once every twelve (12) months or such other period as may be agreed between the Parties taking into account the criticality of this Contract to the Authority and the size and scope of the Supplier's business operations. The Supplier shall promptly provide to the Authority, at the Authority's written request, copies of its Business Continuity Plan, reasonable and proportionate documentary evidence that the Supplier tests its Business Continuity Plan in accordance with the requirements of this Clause 6.3 of this Schedule 2 and reasonable and proportionate information regarding the outcome of such tests. The Supplier shall provide to the Authority a copy of any updated or revised Business Continuity Plan within fourteen (14) Business Days of any material update or revision to the Business Continuity Plan.

6.4 The Authority may suggest reasonable and proportionate amendments to the Supplier regarding the Business Continuity Plan at any time. Where the Supplier, acting reasonably, deems such suggestions made by the Authority to be relevant and appropriate, the Supplier will incorporate into the Business Continuity Plan all such suggestions made by the Authority in respect of such Business Continuity Plan. Should the Supplier not incorporate any suggestion made by the Authority into such Business Continuity Plan it will explain the reasons for not doing so to the Authority.

6.5 Should a Business Continuity Event occur at any time, the Supplier shall implement and comply with its Business Continuity Plan and provide regular written reports to the Authority on such implementation.

6.6 During and following a Business Continuity Event, the Supplier shall use reasonable endeavours to continue to supply the Goods and provide the Services in accordance with this Contract.

INFORMATION AND DATA PROVISIONS

2 Data protection

2.1 The Parties acknowledge their respective duties under Data Protection Legislation and shall give each other all reasonable assistance as appropriate or necessary to enable each other to comply with those duties. For the avoidance of doubt, the Supplier shall take reasonable steps to ensure it is familiar with the Data Protection Legislation and any obligations it may have under such Data Protection Legislation and shall comply with such obligations.

2.2 Where the Supplier is Processing Personal Data under or in connection with this Contract, the Parties shall comply with the Data Protection Protocol.

2.3 The Supplier and the Authority shall ensure that Personal Data is safeguarded at all times in accordance with the Law, and this obligation will include (if transferred electronically) only transferring Personal Data (a) if essential, having regard to the purpose for which the transfer is conducted; and (b) that is encrypted in accordance with any international data encryption standards for healthcare, and as otherwise required by those standards applicable to the Authority under any Law and Guidance (this includes, data transferred over wireless or wired networks, held on laptops, CDs, memory sticks and tapes).

2.4 Where, as a requirement of this Contract, the Supplier is Processing Personal Data relating to patients and/or service users as part of the Services, the Supplier shall:

2.4.1 complete and publish an annual information governance assessment using the NHS information governance toolkit;

2.4.2 achieve a minimum level 2 performance against all requirements in the relevant NHS information governance toolkit;

2.4.3 nominate an information governance lead able to communicate with the Supplier's board of directors or equivalent governance body, who will be responsible for information governance and from whom the Supplier's board of directors or equivalent governance body will receive regular reports on information governance matters including, but not limited to, details of all incidents of data loss and breach of confidence;

2.4.4 report all incidents of data loss and breach of confidence in accordance with Department of Health and/or the NHS England and/or Health and Social Care Information Centre guidelines;

2.4.5 put in place and maintain policies that describe individual personal responsibilities for handling Personal Data and apply those policies vigorously;

2.4.6 put in place and maintain a policy that supports its obligations under the NHS Care Records Guarantee (being the rules which govern information held in the NHS Care Records Service, which is the electronic patient/service user record management service providing authorised healthcare professionals access to a patient's integrated electronic care record);

2.4.7 put in place and maintain agreed protocols for the lawful sharing of Personal Data with other NHS organisations and (as appropriate) with non-NHS organisations in circumstances in which sharing of that data is required under this Contract;

2.4.8 where appropriate, have a system in place and a policy for the recording of any telephone calls in relation to the Services, including the retention and disposal of those recordings;

2.4.9 at all times comply with any information governance requirements and/or processes as may be set out in the Specification and Tender Response Document; and

2.4.10 comply with any new and/or updated requirements, Guidance and/or Policies notified to the Supplier by the Authority from time to time (acting reasonably) relating to the Processing and/or protection of Personal Data.

2.5 Where any Personal Data is Processed by any Sub-contractor of the Supplier in connection with this Contract, the Supplier shall procure that such Sub-contractor shall comply with the relevant obligations set out in Clause 2 of this Schedule 3, as if such Sub-contractor were the Supplier.

2.6 The Supplier shall indemnify and keep the Authority indemnified against, any loss, damages, costs, expenses (including without limitation legal costs and expenses), claims or proceedings whatsoever or howsoever arising from the Supplier's unlawful or unauthorised Processing, destruction and/or damage to Personal Data in connection with this Contract.

4 Information Security

4.1 Without limitation to any other information governance requirements set out in this Schedule 3, the Supplier shall:

4.1.1 notify the Authority forthwith of any information security breaches or near misses (including without limitation any potential or actual breaches of confidentiality or actual information security breaches) in line with the Authority's information governance Policies; and

4.1.2 fully cooperate with any audits or investigations relating to information security and any privacy impact assessments undertaken by the Authority and shall provide full information as may be reasonably requested by the Authority in relation to such audits, investigations and assessments.

4.2 Where required in accordance with the Specification and Tender Response Document, the Supplier will ensure that it puts in place and maintains an information security management plan appropriate to this Contract, the type of Services being provided and the obligations placed on the Supplier. The Supplier shall ensure that such plan is consistent with any relevant Policies, Guidance, Good Industry Practice and with any relevant quality standards as may be set out in the Key Provisions and/or the Specification and Tender Response Document.

4.3 Where required in accordance with the Specification and Tender Response Document, the Supplier shall obtain and maintain certification under the HM Government Cyber Essentials Scheme at the level set out in the Specification and Tender Response Document.

APPENDIX 3

ICO CONTRACTS CHECKLIST GUIDANCE

Full guidance available at:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

Checklists *(Source:* Contracts | ICO))

The contract or other legal act must include terms or clauses stating that:

☐ the processor must only act on the controller's documented instructions, unless required by law to act without such instructions;
☐ the processor must ensure that people processing the data are subject to a duty of confidence;
☐ the processor must take appropriate measures to ensure the security of processing;
☐ the processor must only engage a sub-processor with the controller's prior authorisation and under a written contract;
☐ the processor must take appropriate measures to help the controller respond to requests from individuals to exercise their rights;
☐ taking into account the nature of processing and the information available, the processor must assist the controller in meeting its UK GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
☐ the processor must delete or return all personal data to the controller (at the controller's choice) at the end of the contract, and the processor must also delete existing personal data unless the law requires its storage; and
☐ the processor must submit to audits and inspections. The processor must also give the controller whatever information it needs to ensure they are both meeting their Article 28 obligations.

The contract (or other legal act) sets out details of the processing including:

☐ the subject matter of the processing;
☐ the duration of the processing;
☐ the nature and purpose of the processing;
☐ the type of personal data involved;
☐ the categories of data subject;
☐ the controller's obligations and rights.