WHC (2017) 025

WELSH HEALTH CIRCULAR

Llywodraeth Cymru
Welsh Government

Issue Date: 4 July 2017

STATUS: ACTION

CATEGORY: INFORMATION GOVERNANCE

Title: Guidance on Cyber Security and Information Governance requirements relating to suppliers and the supply-chain

Date of Expiry / Review N/A

For Action by:
Health boards and trusts

Action required by: Immediate

Sender: Dr Andrew Goodall, Director General for Health and Social Services/ NHS Wales Chief Executive

DHSS Welsh Government Contact(s) :
Peter Jones, Deputy Director, Digital Health and Care, Health and Social Services Group, Cathays Park, Cardiff, CF10 3NQ

E-mail: HSS-DHCMailbox@wales.gsi.gov.uk

Enclosure(s): None

WHC 2017/025 – Guidance for Cyber Security and Information Governance requirements relating to suppliers and the supply-chain.

With the increasing prevalence of cyber security threats, NHS Wales needs to ensure the requirements placed on suppliers, and potentially the whole supply chain, remain appropriate to the level of information accessed and/or held by the supplier.

Each organisation must be aware of all third parties holding, accessing or handling staff or patient identifiable data, and ensure that the appropriate level of assurance is evidenced and maintained on an ongoing basis. This should be done in relation to both the data and the contract with the supplier.

All controls should be reviewed on a regular basis and updated to reflect new or amended legislation and the adoption of any revised best practice released by industry experts.

Where the procurement and subsequent delivery of any goods, services or equipment results in one or more of the conditions listed below, appropriate information governance and cyber security controls must be specified in the requirements and must be in place in any resulting commercial or contractual agreements (i.e. within the appropriate set of terms and conditions of contract):

- The supplier, or any party within their supply chain, storing or processing patient, staff or other sensitive personal information; or
- The supplier, or any party within their supply chain, having access to systems on the NHS network which store or process patient, staff or other sensitive personal information.

Procurement teams must engage with appropriate information governance and cyber security specialists in their organisation or at a national level (i.e. within NHS Wales Informatics Service) to ensure that this is achieved/adhered to.

Appendix A - proposes a risk assessment framework against which each third party contract should be assessed and the minimum cyber security standards which should be applied.

Below are recommended minimum considerations relating to Information Governance:

- Compliance with the Wales Caldicott Principles into Practice (CPIP) tool or the England Information Governance Toolkit;
- Robust Data Protection and confidentiality clauses within contracts;
- Compliance with safe harbour or new EU-US privacy shield provisions for any transfers of data to the United States; and
- Compliance with Information Commissioners Office (ICO) guidance on data breach management.

Appendix B and C - provide a summary of the two forms of contract used by NHS Wales Informatics Service (NWIS) for the procurement of IT related

goods and services. Further information on these can be obtained from the NWIS Commercial Services team.

Any queries relating to this circular should be addressed to:

Digital Health and Care
4th Floor
Health and Social Services Group
Cathays Park
Cardiff
CF10 3NQ

E-mail: DHSS-DigitalHealthandCare@Wales.GSI.Gov.UK

Yours sincerely

Dr Andrew Goodall

APPENDIX A

Minimum standards for Cyber Security controls

Below are minimum Cyber Security controls which should be used, depending on the assessed level of risk to systems/data.

1. Not Applicable

In this scenario, the supplier, or any party within their supply chain, does not store, process or have access to patient, staff or other sensitive personal information, nor access to sensitive corporate information.

The supplier, or any party within their supply chain, does not have any form of networked / electronic communication to devices on the NHS Wales network, including connecting into networks/devices when their staff are on NHS sites.

The sorts of contracts this will apply to are likely to be those covering commodity purchases or standard service provisions (e.g. office supplies or the disposal of non-sensitive waste).

This category does not have any specific minimum cyber security control measures, although it is recommended that all suppliers seek to achieve compliance with the Cyber Essentials Scheme, which involves informal self-assessment and commitment to security improvement by the supplier.

2. Very Low (VL)

In this scenario, the supplier, or any party within their supply chain, does not store, process or have access to patient, staff or other sensitive personal information, nor access to sensitive corporate information.

The supplier, or a party within their supply chain, require ad-hoc infrequent access to devices which are connected to the NHS Wales network, or the network itself, which would be achieved through attending sites and connecting directly into the equipment.

The sorts of contracts this will apply to could include maintainers of building management systems, printer maintenance companies, suppliers of specialist non-clinical software, or similar.

Within this category it has been assessed that the cyber security risks to NHS Wales from the contract will be deemed basic (i.e. simple/automated hacking, phishing or spyware) and any attacker is likely to be opportunistic, unskilled and non-persistent. The impact of the theft/loss of data on the NHS organisation (public trust, financial fines, etc.) is likely to be low.

This level requires that the contractor achieves compliance with the Cyber Essentials Scheme, which involves formal self-assessment, declared

compliance by the contractor, and documentation verification by a certified body.

3. Low (L)

In this scenario the supplier, or any party within their supply chain, could have access to very limited amounts of patient, staff or other sensitive personal information which is stored on the NHS network, or very limited access to sensitive corporate information. No such information will be stored by the supplier or any party within their supply chain.

The supplier, or a party within their supply chain, may also require ad-hoc infrequent access to devices which are connected to the NHS Wales network, or the network itself, which would be achieved through attending sites and connecting directly into the equipment. There shall be no means of accessing any systems connected to the NHS network, or any data held on NHS systems remotely.

Within this category it has been assessed that the threat may be slightly more targeted (i.e. involving spear phishing or ransomware and where attackers are semi-skilled but may not be persistent). The impact of the theft/loss of data on the affected individuals and the NHS organisation (public trust, financial fines, etc.) is likely to be low.

This level requires that the contractor achieves compliance with the Cyber Essentials Scheme, which involves formal self-assessment, declared compliance by the contractor, and documentation verification by a certified body.

4. Moderate (M)

In this scenario, the supplier, or a party within their supply chain, have access to greater volumes of, or more sensitive, personal data relating to staff or patients, or access to sensitive corporate information. This information could be stored and processed on the NHS systems/network or by the supplier, or a party within their supply chain.

The supplier, or a party within their supply chain, may also require frequent access to devices which are connected to the NHS Wales network, or the network itself, which is either achieved through attending site and connecting directly, or via an authorised remote access mechanism.

The moderate category applies to contracts where it has been assessed that the cyber risks are more advanced. This will likely apply to contracts involving greater volumes of, or more sensitive, personal data. Attacks are likely to be targeted with the objective of gaining access to a specific asset(s) or to enable a denial of service. The attacker is likely to be persistent, organised and either be skilled or have access to skills (e.g. cyber criminals or hacktivists). The

impact of the theft/loss of data on the affected individuals and the NHS organisation (public trust, financial fines, etc.) is likely to be moderate.

This level requires the contractor to have and maintain Cyber Essentials Plus Certification, which involves formal self-assessment, declared compliance by the contractor, and documentation verification by a certified body.

To achieve and maintain certification, contractors also need to undergo vulnerability testing (by an appropriately qualified / certified external testing organisation), and recertify against Cyber Essentials Plus at least once a year.

5. High (H)

The High Cyber Risk category applies to contracts that are essential to support key clinical capability and those handling bulk sensitive, personal data relating to staff or patients, or access to highly confidential corporate information. This information could be stored and processed on the NHS systems/network or by the supplier, or a party within their supply chain.

The supplier, or a party within their supply chain, may also require frequent access to devices which are connected to the NHS Wales network, or the network itself, which is either achieved through attending site and connecting directly, or via an authorised remote access mechanism.

The high category applies to contracts where it has been assessed that the cyber risks to the contract may be subjected to Advanced Persistent Threats (APT). Attackers at this level will typically be organised, highly sophisticated, well - resourced and persistent. Attacks may be sustained over long periods and may lay dormant for months or years after the initial attack. The impact of the theft/loss of data on the affected individuals and the NHS organisation (public trust, financial fines, etc.) is likely to be significant.

This level requires the contractor to have and maintain Cyber Essentials Plus Certification, which involves formal self-assessment, declared compliance by the contractor, and documentation verification by a certified body.

To achieve and maintain certification, contractors also need to undergo vulnerability testing (by an appropriately qualified / certified external testing organisation), and recertify against Cyber Essentials Plus at least once a year.

In addition to maintaining the Cyber Essentials Plus Certification, the contractor is also expected to evidence working towards certification against ISO/IEC 27001:2013, which provides additional assurance in relation to the contractor’s ongoing commitment to security improvement.

APPENDIX B

Complex Terms and Conditions

Complex Model - Crown Commercial Services (formerly OGC) Model Form Services & ICT Contract for IT solutions and services over a value of £10m. This form of contract reflects current government priorities and recommended ways of doing business and will be refined based on the solution/service that is being procured. However, the key terms are as follows:

Information Governance Key Contractual Terms:

- Compliance with the Data Protection Act and the 7th & 8th Principles;
- Protection of Personal Data;
- In what circumstances Personal Data can be used by the contractor to deliver the agreement;
- Use of data sharing and use in relation to the Freedom of Information Act; and
- Confidentiality of information.

Security Key Contractual Terms

- Compliance of the Contractor's personnel with Security Requirements and Plan and Security Policy;
- Notification by the Authority of any changes to the Security Policy; and
- Compliance with the Security Schedule (Schedule 2.4) and Standards (Schedule 2.3)

There are specific schedules under the Terms and Conditions of Contract, which set out in detail the contractual provisions and obligations for Information Governance and Security.

Schedule 2.3 Standards (Security & IG)
Sets out the standards that must be adhered to in delivering the service e.g. ISO 27001 Security Standard.

Schedule 2.4 Security Requirements (Security)
Sets out the principles of security for the software, the wider aspects of security relating to the solutions/ service creation of the Security Plan and audit and testing of the Security Plan.

Schedule 2.5 Business Continuity (Security)
Sets out the authority's requirements for ensuring continuity of the business processes and operations in circumstances of service disruption or failure and for restoring the service through business continuity and, as necessary, disaster recovery procedures. It also includes the requirement on the contractor to develop, review, test, change and maintain a BCDR Plan in respect of the service.

Schedule 4.2 Commercially Sensitive Information (Information Governance)

This schedule seeks to identify the aspects of the agreement that the contractor considers to be 'commercially sensitive', and therefore the disclosure of which would be detrimental to their business and/or the public interest. In the event of an FOI request this would be considered by the authority but would not in itself stop the authority disclosing the information if it was required to do so.

Schedule 7.2 Audits & Value for Money (IG & Security)
As well as allowing NHS Wales to benchmark charging in the agreement, this contract permits and enables the authority to access the information required to meet its own audit requirements i.e. Security and Information Governance Audits.

Schedule 8.5 Exit Management (Security)
Sets out the principles of the exit and service transfer arrangements that are intended to achieve an orderly transition at the end of this agreement, such as data transfer.

Simple Terms and Conditions (previously called SIMCON)

Simple IT Solution and Services Agreement for solutions which are less complex and have a lower value i.e. under £10m.

Information Governance Key Contractual Terms
Defines Data Processor and Data Controller – Contractor is Data Processer and Authority is Data Controller.

Allows contractor to process data in relation to the delivery of the agreement in accordance with the Data Protection Act, the obligations set out under the agreement and any instructions from the authority from time to time.

Sets out their obligations in relation to the following:

- Compliance with the Data Protection Act;
- Dealing promptly with Authority & Information Commissioner queries in relation to data processing;
- Requests from individuals with regards to accessing their personal data;
- Disclosure or access to unauthorised records;
- Only disclose data to authorised personnel to deliver the contract;
- Technical and organisational security measures to be in place by contractor to ensure that data is not unauthorised accessed or unlawfully processed;
- To ensure that the contractor's actions do not do anything which would cause Data to be transferred outside the European Economic Area;
- Costs need to be borne by the contractor in relation to any updated to the Data Protection Act to ensure that they are compliant;
- Ensure that they keep data confidential unless where disclosure is expressly permitted;
- Termination; on or before the date when the Agreement terminates or expires, the Contractor must ensure that all documents/records that are in the contractor's possession or control either must be permanently deleted;
- On termination the Contractor shall cease to use Authority Data; and
- Audit of data by the Authority is provided for in the Agreement.

FOIA

- Use of data sharing and obligations to adhere to in relation to the sharing of data in relation to the Freedom of Information Act.

Security Key Contractual Terms

- Compliance of the Contractor's personnel with Security Requirements, Plan and Security Policy;
- The Contractor will adhere to the NHS Wales Security requirements including the penetration testing of the solution on go live and annually via a CLAS Consultant and adherence to CHECK Standards;

- Security Audits of the solution by the Authority are provisioned;
- application of security patches and adherence to the Authority's Security Policy;
- All Servers deployed under the contract are to be hardened;
- Maintenance of a plan to manage a cybersecurity incident; and
- No data leaving NHS Wales Network without written consent.