Title	**2017-19 Data Security and Protection Requirements**
Author	LOCSU/OC
Document Purpose	Guidance for implementing the new data security and protection requirements
Publication Date	February 2018
Target Audience	All providers of eye health services contracting via the NHS Standard Contract.
Contact details	LOCSU 020 7549 2051 info@locsu.co.uk Optical Confederation http://www.opticalconfederation.org.uk/contact-us/contact-us

Summary

This LOCSU/OC guidance explains the requirements for implementing new data standards for the optical sector for 2017-18, going into 2018-19.

These standards do not apply to GOS contracts.

Background

Data security and protection is firmly on the NHS and Government's agenda after some recent high-profile cyber and information security incidents. In November 2014, the Secretary of State for Health appointed Dame Fiona Caldicott as national data guardian for health and care; in July 2017 the Government accepted the ten data security standards recommended by Dame Caldicott. https://www.gov.uk/government/news/national-data-guardian-ndg-statement-ongovernment-response-to-the-ndg-review.

In November 2017 the Department of Health (DH) published new guidance: 2017-18 Data Security and Protection Requirements.

This has been summarised here by LOCSU/OC for use by optical providers of locally commissioned services under the NHS Standard Contract.

General Data Protection Directive (GDPR)

Please be aware that wider data changes will take effect from 25 May 2018, when the General Data Protection Directive (GDPR) applies. You should therefore read this guidance in conjunction with Optical Confederation guidance on changes to data protection law.

http://www.opticalconfederation.org.uk/downloads/data-protection-and-gdpr-guidance--final.pdf

Who these requirements apply to

The *2017-8 Data Security and Protection Requirements* are part of wider data security and protection requirements detailed in the NHS Standard Contract.

This means that all providers of locally commissioned eye health services under an NHS Standard Contract—such as LOC companies (also known as Primary Eyecare Companies) or individual contractors—are required to meet these new data and security requirements.

LOC companies need to ensure that their subcontractor optical practices which deliver services on behalf of the LOC company also comply with these requirements.

2017-18 Data Security Requirements

There are three leadership obligations under which the data security standards are grouped:

Leadership Obligation One – People

1. **Senior Level Responsibility**

   LOC companies and optical subcontractors/contractors must have a named person in a management role responsible for data and cyber security in the company/practice. This person will have the lead role to ensure that the data security and protection standards are implemented. The DH Data Security and Protection Requirements guidance recommends that this named individual is the same person as the Senior Information Risk Owner (SIRO). A SIRO is already a Standard Contract requirement.

   The Optical Confederation strongly recommends, however, that you do not give this named person the title Data Protection Officer (DPO). This is because a DPO is a specific role defined in the GDPR with very specific legal responsibilities and it could create an additional regulatory burden, resulting

in unnecessary work for your business if you appoint a DPO when you do not need to.

While CCGs may also offer or provide support on cyber security issues, this does not change the fact that each optical contractor is ultimately responsible for ensuring the rules are followed. Also, it should not be assumed that advice from CCGs is invariably correct in respect to optical practices: their assumption can be that requirements for one profession (e.g. GPs) apply to another, when this is not necessarily the case.

If in any doubt, contractors should contact their or LOC or Optical Confederation representative body (see 'Useful Contacts'). LOCs should contact LOCSU.

2. Completing the Information Governance Toolkit v14.1 by 31st March 2018

All those who have previously completed the Information Governance Toolkit (IGT) and/or have been instructed to by their commissioning body should complete it again for the financial year 2017-18 if they have not already done so (deadline 31st March 2018).

This is the last year that the IGT will be in place before it is replaced by the new Data Security and Protection Toolkit (DSPT) from 2018-19 onwards. The DSPT will be designed to measure an organisation's progress against the ten data targets. LOCSU and the Optical Confederation will be updating their Information Governance (IG) guidance and Quality in Optometry (QiO) to reflect the DSPT requirements for completion in the financial year 2018-19. In the meantime, discussions about how this will affect optical practices are still taking place with NHS Digital.

3. **Prepare for the introduction of the General Data Protection Regulation in May 2018**

   The OC guidance explains what you should do now to prepare for the GDPR. It will be updated as and when the Government and the Information Commissioner's Office (ICO) provide further advice.

4. **Training Staff**

   For the current IGT for 2017-18, the existing IG materials on QiO are still relevant: https://www.qualityinoptometry.co.uk/

   Note, for services commissioned through the Standard Contract, QiO checklists and associated IG training materials are separated by contracting scenario (for example, LOC company, LOC company subcontractor, and practices contracting directly with CCGs). These materials can also be found within the 'Policies' section of QiO.

   Once the IGT has been replaced by the DSPT from April 2018 LOCSU and the OC will develop a new suite of IG support materials for users. This will include optical sector specialist video training.

Leadership Obligation Two – Processes

5. **Acting on CareCERT advisories**

   The Department of Health have commissioned NHS Digital to develop a Care Computer Emergency Response Team (CareCERT). CareCERT will offer advice and guidance to support health and social care organisations to respond effectively and safely to cyber security threats.

   However, this does not currently apply to optical practices. This is because at present the system can only be accessed via an N3 connection, which optical practices do not have. Accordingly, DH states that 'Action might include

understanding that an advisory is not relevant to your organisation's systems and confirming that this is the case.'

6. **Continuity planning**

   The NHS Standard Contract conditions require a comprehensive business continuity plan to be in place to respond to data and cyber security incidents.

   Template business continuity and disaster recovery plans are available within QiO assigned to the relevant Standard Contract questions, split by contracting scenario, or found within the 'Policies' section.

7. **Reporting incidents**

   Template serious incident reporting policies for data security breaches and near misses are available within QiO assigned to the relevant Standard Contract questions, split by contracting scenario, or found within the 'Policies' section. These policies include reporting procedures.

   As noted above (5), the requirement to report data security incidents and near misses to CareCERT does not currently apply to the optical sector.

Leadership Obligation Three – Technology

8. **Unsupported systems**

   Practices/providers operating under the Standard Contract must:

   - Identify unsupported systems (including software, hardware and applications); and
   - Have a plan in place by April 2018 to remove, replace or actively mitigate or manage the risks associated with unsupported systems.

   Unsupported systems are those:

- With no product support
- No patch updates
- No bug fixes
- Potentially no anti-virus or software updates
- Old hardware which is hard to use and repair
- Eventually these systems become vulnerable to attack and compromised
- Compromised systems mean information and logins are vulnerable to theft, and a compromised machine can be used to attack other machines.[1]

'Systems' may relate to operating systems (software that manages computer hardware and software resources) and provides common services for computer programs, or specialist optical systems. An example of a well-known operating system that no longer has security updates provided for it is Microsoft's Windows XP.

If you have questions or concerns regarding the status of your systems, you should contact the provider.

A good practice guide for managing the risk of unsupported systems is available from NHS Digital and should be read and acted upon where necessary:

https://www.digital.nhs.uk/media/31701/NHS-managing-the-risk-of-unsupported-platforms-Good-practice-guide/pdf/Managing_the_Risk_of_Unsupported_Platforms_-_Good_Practice_Guide_230517

[1] http://med.stanford.edu/irt/security/connecting/end-of-life-systems.html

9. On-site Assessments

In the unlikely event of a request by NHS Digital to conduct a practice/company cyber and data security assessment you must:

- Comply with this
- Act on the outcome of the assessment, including any recommendations, and share the outcome with your commissioner(s).

It is probable that these requests will be aimed at larger organisations than optical practices/LOC companies, but you need to be aware of the possibility.

10. Checking Supplier Certification

Your IT suppliers must have the appropriate certification. There are a variety of these listed by the DH:

- ISO/IEC 27001:2013 certification
- Cyber Essentials (CE) certification
- Cyber Essentials Plus (CE+) certification
- Digital Marketplace

If you are unsure check with your commissioner and software provider that the correct certification for the services is in place. CCGs have a duty under the data standards to ensure that their providers' IT systems are compliant with the required standard for the service.

Further information

Practices should also refer to the following for assistance with complying with the data standards:

- https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
- https://digital.nhs.uk/cyber-security/policy-and-good-practice-in-health-care/good-practice-guides

Useful contacts

LOCs/LOC companies - Richard Knight: richardknight@locsu.co.uk

ABDO members - Katie Docker: kdocker@abdo.org.uk

AOP members - policy@aop.org.uk

FODO members – optics@fodo.com

Key dates

- February 2018: All organisations that have previously completed IGTs will be granted access to the DSPT to begin preparations for completion in 2018-19
- 31st March 2018: Contractors required to complete the IGT must do so by this date
- From April 2018: the DSPT will be live and contractors will have one year to complete it from this date. Further guidance will be released by the NHS. LOCSU/OC will be producing optical sector specific guidance for completion for 2018/19
- May 2018: EU General Data Protection Regulation (GDPR) and Security of Network and Information Systems Directive comes into force. The OC guidance has produced guidance on this: http://www.opticalconfederation.org.uk/downloads/data-protection-and-gdpr-guidance--final.pdf
- 31st March 2019: DSPT deadline for completion.

LOCSU/Optical Confederation

February 2018