ukcloud health

Making transformation happen.

The Data Security and Protection (DSP) Toolkit

The National Data Guardian, Dame Fiona Caldicott, has compiled and recommended a framework of "10 data security standards" which will be applicable to all health and care organisations. It will apply to NHS Providers, Clinical Commissioning Groups, General Practices, Local Authorities and Social Care Providers. It will also place responsibility on these organisations to fully assess the compliance of any third-party suppliers who manage or process data on their behalf.

This new approach, which will assure that healthcare organisations are meeting their statutory obligations on information security and data protection, will be delivered using a new Data Security and Protection (DSP) Toolkit, which replaces the long established existing Information Governance (IG) Toolkit. The DSP Toolkit requires health and care organisations to undertake preparations for compliance with the EU General Data Protection Regulation, which takes effect on 25th May 2018.

DSP toolkit guidance

The DSP Toolkit is arranged into three categories of leadership obligations: **people, process and technology**.

PEOPLE

The human element of cyber security is often underplayed when organisations are planning for change. The DSP Toolkit highlights the need to improve the 'people' element to reduce organisational vulnerabilities:

- **Senior level responsibility:** One senior executive, preferably a member of the organisation's board, should be responsible for data and cyber security. Ideally, this person will also be the senior information risk owner.
- **IG Toolkit v14.1:** In 2017/18 organisations will still be required to comply with the IG Toolkit v14.1, to a minimum of level two. The DSP Toolkit will be released in April 2018, replacing the IG Toolkit.
- **Complete the GDPR checklist:** The GDPR comes into force in May 2018, replacing the Data Protection Act 1998 (DPA) as the regulatory standard for any organisation that processes the personal data of EU residents. NHS Digital will publish a checklist of requirements for GDPR compliance. To achieve DSP Toolkit compliance, all organisations will need to complete that checklist to demonstrate adherence to the Regulation.
- **Training staff:** All staff will be required to complete appropriate data security and protection training in line with the remit of their role. From 2018, NHS Health Education England training courses will include cyber security training modules and the requirements of the DSP Toolkit.

PROCESS

The DSP Toolkit identifies steps that need to be taken to prevent and mitigate the effects of a data breach:

- **Acting on CareCERT advisories:** CareCERT advisories notify healthcare organisations of immediate and upcoming cyber security threats. Under the DSP Toolkit, organisations will be required to act on these notifications and, for the more severe threats, confirm within 48 hours that plans are in place to act on them.
- **Business continuity planning:** The DSP Toolkit requires organisations to have a comprehensive plan to ensure business continuity while recovering from an event, such as a data breach or cyber attack.
- **Reporting incidents:** All data security incidents will need to be reported to CareCERT in line with reporting guidelines.

TECHNOLOGY

Technology is a key element in achieving effective cyber security. The DSP Toolkit identifies the technology controls that need to be in place to support data security and protection.

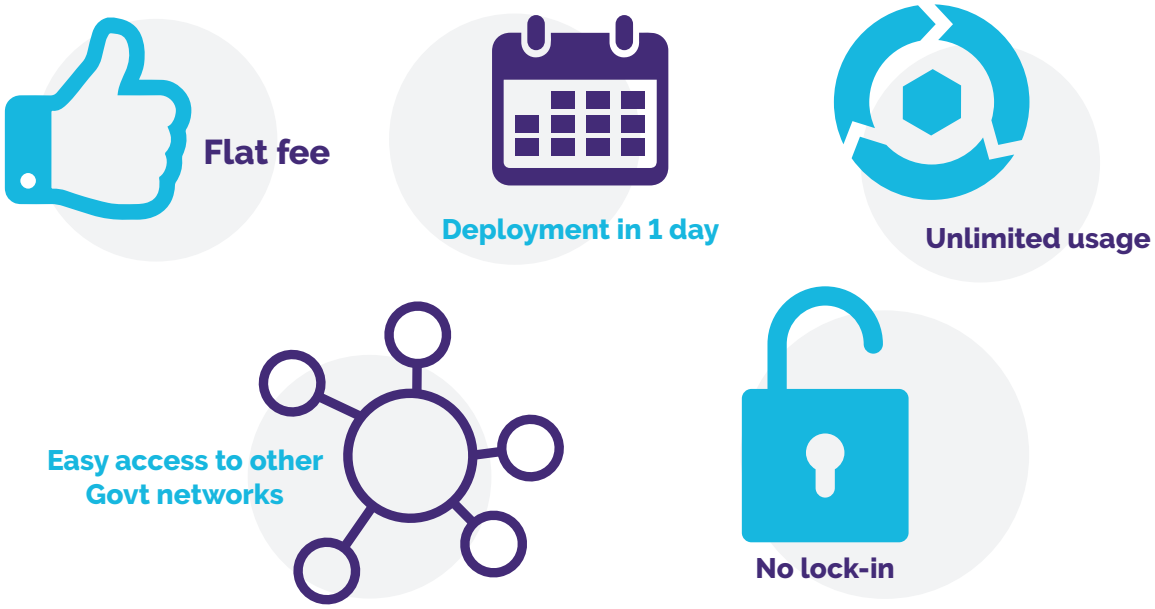
Activities include:

- **UNSUPPORTED SYSTEMS** - the identification and removal of all unsupported systems (hardware, software and applications)
- **ON-SITE ASSESSMENTS** - The conduct of on-site security assessments (and remediating any findings)
- **SUPPLIER CERTIFICATION** - Checking the certification status of all third-party suppliers against a framework of certifications. Supplier certification frameworks include ISO/IEC27001:2013 (by a UKAS accredited organisation), Cyber Essentials and Cyber Essentials Plus, or services available through the UK Government's Digital Marketplace.

UKCloud Health is pleased to confirm that it already holds these certifications, which support its provision of secure, easy to use sovereign assured cloud services into healthcare communities.

John Godwin, Director of Compliance and Information Assurance at UKCloud Health noted *"UKCloud Health's no-compromise approach to robust data security and technical resilience has allowed us to develop a significant portfolio of healthcare customers. Our ability to demonstrate our competencies and security controls is essential in supporting them to select credible cloud services, which meet the requirements of both the new DSP Toolkit and the imminent General Data Protection Regulation".*

5 key reasons to choose UKCloud Health for HSCN



ukcloud health

E info@ukcloudhealth.com
T 01252 303 300
ukcloudhealth.com