What is the Data Security Standards?

All NHS digital, data and technology services should achieve the Data Security Standards (DSS) required through the Data Security and Protection Toolkit (DSPT), which is made up of ten standards. The DSPT retains the general principle that organisations should demonstrate that they can be trusted with the confidentiality and security of personal information. It also supports organisations to meet the requirements of new legislation including the likes of the General Data Protection Regulation (GDPR) and Network and Information Systems (NIS) Directive. It is important to note that the DSPT will continue to evolve over time to reflect emerging threats, changing policy and future legislative requirements.

The ten Data Standards are an overarching framework; each standard is broken down into evidence items called assertions which cover the detail required to meet each standard. They cover more than technology, encompassing people and process:

Standards 1, 2, 3	**People**	• Staff understand and ensure the processes for the secure management and storage of personal confidential data and that it is only shared lawfully and understand their personal accountability. • Staff must complete and pass a mandatory annual data security test.
Standards 4, 5, 6, 7	**Process**	• Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. • Processes are reviewed annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security. • Cyber-attacks against services must be identified and resisted, and continuity plans in place to respond to threats to data security and is tested annually as a minimum.
Standards 8, 9, 10	**Technology**	• No unsupported operating systems, software or internet browsers are used within the IT estate. • A strategy is in place to protect IT Systems from cyber threats using a proven cyber security framework which is reviewed annually. • IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the Data Security Standards.

How should you be responding to the Data Security Standards?

UKCloud Health has developed mature capabilities with its comprehensive framework addressing information security, data protection and governance. Alongside the requirements within, further information is available in our responses to NHS digital, data and technology standards framework and the Minimum Cyber Security Standard sections of this web page.

Standard	Customer responsibilities	What is UKCloud Health's position	More information
1. Personal Confidential Data	Staff ensure that personal confidential data is handled, stored and transmitted securely, and personal confidential data is only shared lawfully. If you choose to use a cloud service provider, you will need to ensure that they can also protect personal confidential data (evidenced by their completion of a satisfactory DSPT).	Customers who are authorised users of the NHS Digital DSPT website can search for UKCloud Ltd (8J561) to view our latest DSPT assessment online. This document is also available on request through our website.	UKCloud's comprehensive G-Cloud Evidence Pack containing assurance information is available on request Comprehensive Assurance page on our website provides assurance information and evidences our approach to data security. Ensuring the security of personal data processing - blog written by UKCloud's Director of Compliance & Information Assurance.
2. Staff Responsibilities	All staff understand their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches. If you choose to use a cloud service provider, you will need to ensure that their staff responsibilities have been clearly defined (evidenced by	Customers who are authorised users of the NHS Digital DSPT website can search for UKCloud Ltd (8J561) to view our latest DSPT assessment online. This document is also available on request through our website.	System Interconnect Security Policy (SISP) page on our website provides an overview of the SISP and explains the respective roles and responsibilities of the customer and the cloud service provider (UKCloud).

	their completion of a satisfactory DSPT).		
3. Annual security training	All staff complete appropriate annual data security training and pass a mandatory test. If you choose to use a cloud service provider, you will need to ensure that their staff complete annual data security training (evidenced by their completion of a satisfactory DSPT).	Customers who are authorised users of the NHS Digital DSPT website can search for UKCloud Ltd (8J561) to view our latest DSPT assessment online. This document is also available on request through our website.	We comply with the following ISO standard and can provide certificates on request: Information Security Management (ISO27001) The highest standards for the UK Public Sector page on our website explains our approach and shows adherence to compliance frameworks.
4. Managing data access	Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. If you choose to use a cloud service provider, you will need to ensure that they have controls in place to ensure that access to personal confidential data by their personnel is properly managed (evidenced by their completion of a satisfactory DSPT).	Customers who are authorised users of the NHS Digital DSPT website can search for UKCloud Ltd (8J561) to view our latest DSPT assessment online. This document is also available on request through our website.	UKCloud's comprehensive G-Cloud Evidence Pack containing assurance information is available on request. GDPR page on our website explains the link between GDPR and cloud services and provides information on how UKCloud are GDPR compliant.

5. Process reviews	Processes are reviewed at least annually to identify and improve processes which have caused breaches and compromised data security. If you choose to use a cloud service provider, you will need to ensure that their processes are subject to regular review on at least an annual basis (evidenced by their complete on of a satisfactory DSPT).	Customers who are authorised users of the NHS Digital DSPT website can search for UKCloud Ltd (8J561) to view our latest DSPT assessment online. This document is also available on request through our website.	System Interconnect Security Policy (SISP) page on our website provides an overview of the SISP and explains the respective roles and responsibilities of the customer and the cloud service provider (UKCloud).
6. Responding to Incidents	Cyber-attacks against services are identified and resisted and NHS Digital Data Security Centre security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection. If you choose to use a cloud service provider, you will need to ensure that they have the capability (for example, by protective monitoring) to detect cyber incidents and notify you promptly (evidenced by their completion of a satisfactory DSPT).	Customers who are authorised users of the NHS Digital DSPT website can search for UKCloud Ltd (8J561) to view our latest DSPT assessment online. This document is also available on request through our website.	The highest standards for the UK Public Sector page on our website explains our approach and shows adherence to compliance frameworks. We comply with the following ISO standards: • Information Security Management (ISO27001) • IT Service Management (ISO2000) Monitoring the UKCloud platform - Knowledge Centre article, provides information on how we monitor our platform, including our security incident monitoring system that scans for potential security incidents 24 hours a day.

			The benefits of protective monitoring blog reviews the need for protective monitoring and the preventative measures that can be taken to avoid and resolve vulnerabilities.
7. Continuity Planning	A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, tested annually. If you choose to use a cloud service provider, you will need to ensure that they have an effective continuity plan in place which is subject to testing on at least an annual basis (evidenced by their completion of a satisfactory DSPT).	Customers who are authorised users of the NHS Digital DSPT website can search for UKCloud Ltd (8J561) to view our latest DSPT assessment online. This document is also available on request through our website.	Sites, Regions and Zones – Knowledge Centre article explaining how customers can design applications that are highly resilient. The Disaster Recover as a Service page on our website provides information on the options, features and benefits of DRaaS for customers. This case study shows how Zerto technology can help restore services following cyber security breaches UKCloud's comprehensive G-Cloud Evidence Pack containing assurance information is available on request.
8. Unsupported Systems	No unsupported operating systems, software or internet browsers are used within the IT estate. If you choose to use a cloud service provider, you will need to seek their confirmation that no unsupported operating systems, software or internet browsers are used within their IT estate (evidenced by their	Customers who are authorised users of the NHS Digital DSPT website can search for UKCloud Ltd (8J561) to view our latest DSPT assessment online. This document is also available on request through our website.	UKCloud provides a cloud assessment service to help understand what customers currently have in their estate and recommends how they can take advantage of our CyberScore service to identify if any unsupported or incorrectly patched software exists within their infrastructure. UKCloud was one of the first organisations to have successfully achieved both Cyber Essentials and Cyber Essentials Plus accreditations and has consistently maintained these certifications.

	completion of a satisfactory DSPT).		UKCloud has been assessed in five key control areas: boundary firewalls and internet gateways, secure configuration, access control, malware protection and patch management. The Accreditations and certifications page on our website provides information about our compliance framework and current accreditations.
9. IT Protection	A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework reviewed annually. If you choose to use a cloud service provider, you will need to ensure that they have a cyber security strategy in place (evidenced by their completion of a satisfactory DSPT).	Customers who are authorised users of the NHS Digital DSPT website can search for UKCloud Ltd (8J561) to view our latest DSPT assessment online. This document is also available on request through our website.	The benefits of protective monitoring blog reviews the need for protective monitoring and the preventative measures that can be taken to avoid and resolve vulnerabilities. We comply with the following ISO standards: • Information Security Management (ISO27001) • Security Controls for Cloud Services (ISO27017) • Personal Data in the Cloud Security (ISO27018) All services undergo an annual NCSC-approved ITSHC CHECK Test. UKCloud's comprehensive G-Cloud Evidence Pack containing assurance information is available on request.

10. Accountable Suppliers	IT suppliers are held accountable via contracts for protecting the personal confidential data they hold. If you choose to use a cloud service provider, you will need to ensure that an appropriate contract is in place that provides for the protection of personal confidential data (evidenced by their completion of a satisfactory DSPT).	Customers who are authorised users of the NHS Digital DSPT website can search for UKCloud Ltd (8J561) to view our latest DSPT assessment online. This document is also available on request through our website.	UKCloud's comprehensive G-Cloud Evidence Pack containing assurance information is available on request.