NHS

Data Storage & Security Guide

101 DATA SOLUTIONS

Executive Summary

The medical industry is rapidly growing more digital by the day. From patient records to radiological images, data handling has become increasingly digitised.

Unfortunately, most NHS storage facilities were not designed for storing this much data, so the medical industry continues to face challenges with managing and storing data efficiently.

The importance of data storage in medicine will only continue to rise. With so much information being stored digitally in the medical world, it's becoming increasingly crucial for NHS Trusts to implement processes enabling them to improve their data management.

The danger with any business or industry relying heavily on IT infrastructure is that they can become completely reliant on these systems when something goes wrong.

Therefore, any organisation looking to store sensitive information must have a backup system if things go wrong. This guide identifies the key areas NHS Trusts need to consider regarding their data.

The team at 101 Data Solutions

101 DATA SOLUTIONS

Data Storage

How does the NHS store data?

Electronic Health Records

Electronic health records are traditionally kept on-premise or in a private or hybrid cloud environment. However, for ease, security and flexibility, it is recommended that a single cloud storage solution can be used for all EHR systems, regardless of who owns or operates the system.

DICOM Storage

DICOM provides a consistent method of storing, transmitting, and receiving image-related data. Ensuring compliance with DICOM ensures that any device or software application can understand your imaging data, including images, reports, and study parameters.

For storing and archiving DICOM data, there are several data storage solutions. These include the following:

- Single file storage is the simplest and most common method for storing DICOM data. The entire file is stored in a single file with no directory structure. The file is typically stored on a network share or in the cloud.

Data Storage

- **Directory storage**: this is the default storage method used by many PACS systems. Patient images are stored in a directory structure under a single folder, typically as a folder within a folder.

- **Database storage**: used for storing images and related information. They can be stored on a single server or distributed. Data is typically stored in a single file or table.

- **DICOM Archive Storage**: used for storing images from multiple sources such as scanners, PACS, or other imaging devices. DICOM Archive files are typically stored as a single folder or database on a NAS, SAN, or a DICOM Archive. DICOM Archive files can also be stored in the cloud.

- **Cloud storage**: a suitable option for storing DICOM data. It offers high availability, scalability, and security.

101 DATA
SOLUTIONS

Data Storage

Best Practice Tips

- Invest in data storage solutions designed to store 4K resolution video files.
- Collaborate with IT service providers to upgrade NHS data storage facilities.
- Outsource data storage services to reduce the workload on NHS data storage facilities.
- Create a transition strategy to adopt new technologies and transition away from legacy systems.
- Conduct a Data Audit. Audit data currently stored in NHS servers to determine how much data is being held, why it is being stored, and the cost of storing it. This way, you can learn how to reduce data storage needs and make better decisions about transitioning.
- Choose data storage solutions that are designed for storing large amounts of data. If you decide to upgrade your current systems, choose systems that can store large amounts of data efficiently.
- Outsource data storage services. You can outsource data storage services if your healthcare organisation is not ready to invest in new data storage solutions.

101 DATA SOLUTIONS

Data Backup & Cybersecurity

How does the NHS keep data secure?

Often organisations implement a multi-layered security approach, including firewalls and antivirus software. They also may have an intrusion detection system (IDS) in place to actively monitor and identify potential attacks.
A data loss prevention (DLP) solution is another standard security measure. It helps an organisation protect sensitive data by identifying, monitoring, and controlling data flow to and from sensitive systems. NHS Trusts should reassess their existing data protection practices to meet the necessary requirements.

Best Practice Tips

- Migrate to modern antivirus software: healthcare providers should also consider moving away from legacy antivirus software and adopting a modern approach to security.

- Take a look at your network infrastructure: during this process, NHS Trusts should look to implement technology that offers high availability, scalability, and resiliency. They should also work to strengthen network perimeters and consider the adoption of next-generation firewalls, intrusion detection systems, and virtual private networks.

- Assign new certificates to web apps and services to strengthen encryption across their networks.

Data Backup & Cybersecurity

These certificates identify and authenticate devices, users, and systems across the internet. They are often used to transmit sensitive data across the internet securely. When these certificates are compromised, hackers can use them to sign their malicious code, which makes it much harder to identify and shut down a cyberattack. NHS Trusts can safeguard against this by using certificates with a high level of encryption, rotating certificates regularly, and monitoring for signs of malicious activity across their networks.

- Implement an Intrusion Detection System: IDS systems are designed to identify malicious activity across networks and can help identify cyber threats before they result in a data breach. For example, intrusion detection systems can be beneficial in identifying ransomware attacks and other types of malware infections that would lock down sensitive data and demand a ransom payment to release it.

- Update your operating systems and software: keep an eye on your software and operating systems and keep them updated with the latest versions and patches. Trusts should look to implement a patch management strategy that includes frequent patching and upgrading software across their entire network. Outdated software and operating systems no longer supported by their manufacturers make them more susceptible to being hacked.

Data Backup & Cybersecurity

- Review and harden your network perimeters to ensure that attackers cannot breach the networks or gain access to sensitive data. Network perimeters can be strengthened through the implementation of security technologies, like firewalls, VPNs, IDSs, and network segmentation. NHS Trusts should also look to implement security best practices across their entire network, including the use of strong passwords and two-factor authentication, as well as the use of encryption across all sensitive data.

- Create a culture of security awareness training for employees. Cybersecurity threats are constantly evolving, and employees must be kept up to date on the latest forms of attack and be given resources to help them identify and prevent threats on their networks. When employees know what to look out for, they can play an important role in protecting sensitive data and preventing cyberattacks.

101 DATA
SOLUTIONS

Data Solutions that protect and enhance your organisation

101 Data Solutions know how important data management is to your organisation.

We understand that aligning the correct technologies is crucial to your success, but choosing the right solution can be difficult.

At 101 Data Solutions, we specialise in helping you understand your data: what it is, where it resides, and how to protect and store it.

Our friendly team will work closely with you and strive to understand your needs. Through consultancy and assessment of your environment, we'll then discuss appropriate high-quality products and solutions from leading brands, helping you to choose what's right for you.

We also offer installation services and a wide range of maintenance support options for your equipment.

0117
4350485

101 DATA
SOLUTIONS

Broad Quay House
Prince Street
Bristol City Centre
BS1 4DJ