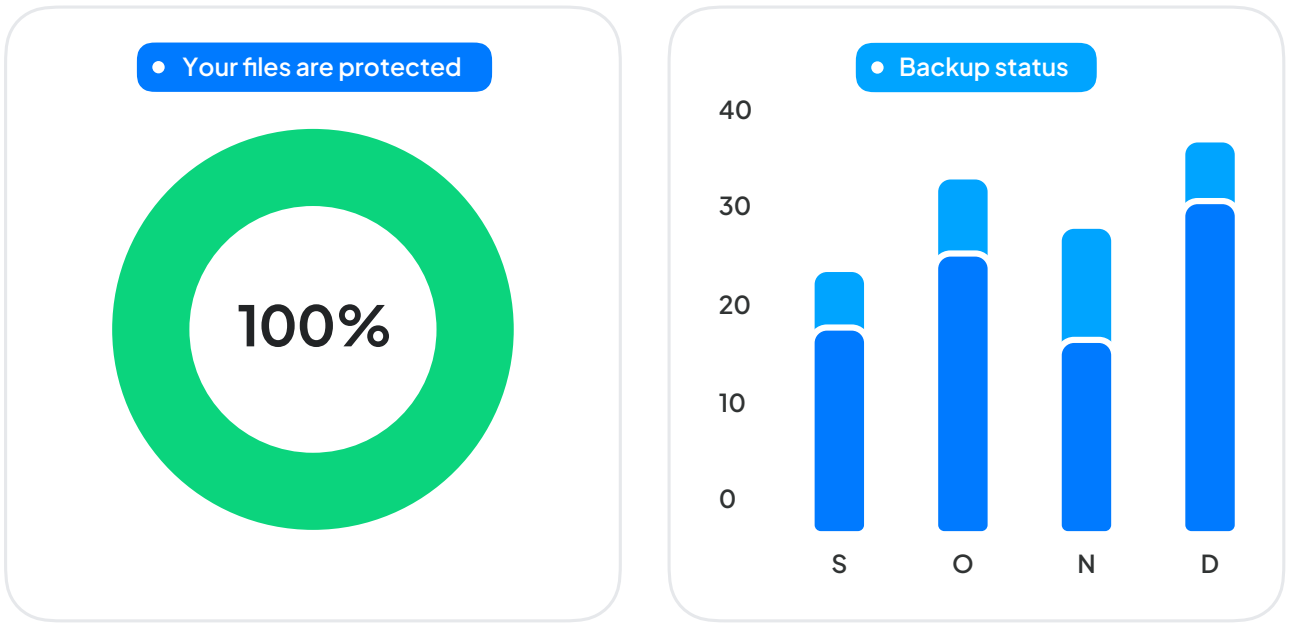
BACKUPVAULT

Data backup requirements in the healthcare industry: What must we legally back up?



Introduction

Protecting sensitive data is paramount for your healthcare organisation to ensure compliance with regulations and the security and continuity of your operations. Yet, with the vast amount of data spread throughout your organisation, determining which specific data to back up can be daunting.

In this comprehensive guide, we'll address a key question: "What data do I legally need to back up as a healthcare organisation?"

We'll shed light on your legal obligations and provide best practices to safeguard your patients' sensitive information.

What is data backup, and why is it important for the healthcare industry?

Backup is a crucial process that involves creating copies of critical data and files to safeguard them from potential loss or damage. In the healthcare industry, where the availability and integrity of patient information are paramount, backup plays a vital role. It ensures that critical medical records, test results, treatment plans, and other essential health data are protected and readily accessible.

By regularly backing up your data, your organisation can minimise the risk of data loss due to hardware failure, natural disasters, or human error. This ensures continuity of care, enhances patient safety, and maintains the integrity of your medical operations.

Additionally, data backup is of utmost importance in protecting the healthcare industry from the ever-growing threat of ransomware attacks.

One significant example is the 2017 NHS ransomware attack. This cyberattack affected the UK's National Health Service (NHS), crippling its IT systems and disrupting patient care. The attack resulted in cancelled appointments, delayed treatments, and an overall disruption of healthcare services. Having reliable backups in place enables healthcare organisations to protect themselves from such attacks by ensuring that critical data can be restored quickly and effectively.

Overall, in a rapidly evolving healthcare landscape and the rise of new technologies, having robust backup systems and practices is essential for preserving patient information confidentiality, availability, and reliability.

What data must I back up?

In the UK, the Care Quality Commission (CQC) plays a significant role in overseeing and regulating various healthcare organisations, including hospitals, dentists, care homes, and more.

To ensure compliance and maintain patient data confidentiality, healthcare organisations must implement robust data backup procedures to protect their organisation's personal information. The personal data that must be backed up includes:

- **Electronic Health Records (EHRs):** EHRs contain comprehensive patient information, including medical histories, test results, diagnoses, and treatment plans.
- **Communication logs and correspondence:** Emails, communication logs, and correspondence related to patient care, referrals, and administrative purposes should be backed up.
- **Patient information:** Backing up patient demographic data such as names, addresses, contact numbers, and emergency contact details ensures that communication channels remain open and patient care remains uninterrupted.
- **Administrative data:** Employee records, operational information, scheduling details, and any other data necessary for the smooth functioning of the healthcare organisation.
- **Research and clinical data:** For healthcare organisations involved in research and clinical trials, backing up research data, experimental results, and patient participation records is essential.
- **Financial records:** Healthcare organisations handle financial data, including insurance details, billing records, and payment information.

Data protection laws for healthcare organisations

As part of their regulatory requirements, healthcare organisations are obligated to adhere to data protection laws and guidelines set forth by key entities, including:

GDPR

GDPR is the pivotal law governing the handling of personal data, encompassing sensitive information about individuals. It was implemented in May 2018, alongside the Data Protection Act 2018. All organisations, including healthcare organisations, must meet the regulations laid out by GDPR, including:

- **Minimise data:** Process the least personal data necessary to fulfil your purpose.
- **Retention period:** Retain personal data only for as long as required, considering the purpose for which it was collected.
- **Breach reporting:** Promptly report any security breaches or incidents that may compromise the security of personal data.
- **Respect rights:** Understand and respect the rights of individuals whose data you collect, including access, rectification, and erasure.
- **Lawful processing:** Conduct assessments to ensure legal & legitimate processing of personal data.
- **Data security:** Take appropriate measures to protect personal data and identify potential privacy risks.
- **Data protection officer:** Determine if appointing a data protection officer is necessary for your organisation.
- **Consent consideration:** Evaluate whether consent is necessary from the individuals whose data you seek to collect.
- **Transparency:** Be transparent and open about how you process personal data, including providing clear information to individuals.

The National Data Guardian Act

The National Data Guardian (NDG) emphasises the importance of data backup as part of its recommendations on data security. The NDG advises healthcare organisations to implement robust backup measures to ensure the availability and confidentiality of patient data. These include:

- Share data only for "lawful and appropriate" reasons.
- Limit access to personal information to authorised personnel.
- Develop a strategy for IT system protection based on established frameworks like Cyber Essentials.
- Develop a strategy for IT system protection based on established frameworks.
- Establish a plan for addressing data security threats.
- Avoid using unsupported older software.
- Hold IT suppliers accountable through contracts that align with the National Data Guardian's standards.
- Care, referrals, and administrative purposes should be backed up.

NHS Digital Guidance

NHS Digital provides general guidance to healthcare organisations regarding health data backup practices. Here are some key principles and recommendations that healthcare organisations typically follow when it comes to health data backup:

- **Regular data backup:** Establish routine backup procedures to ensure the availability and recoverability of critical data in the event of data loss or system failure.
- **Off-site storage:** Store backup data off-site or in secure remote locations to minimise the risk of data loss due to physical damage or on-site incidents.
- **Data retention:** Determine appropriate retention periods for backed-up data, considering legal, regulatory, and business requirements.
- **Encryption and security:** Data backups should be encrypted and secured to protect sensitive information from unauthorised access or breaches.
- **Testing and verification:** Regular testing of the backup process and conducting restoration drills.
- **Documentation and policies:** Document backup processes, including procedures, responsibilities, and policies.

Information Commissioner's Office (ICO)

The ICO is an independent authority responsible for enforcing data protection laws and promoting good information handling practices. The ICO outlines principles and guidelines that organisations, including healthcare providers, must follow when processing personal data. These principles include:

- **Purpose limitation:** Personal data should only be collected for specified, explicit, and legitimate purposes.
- **Data minimisation:** Organisations should only collect and retain the minimum amount of personal data necessary to achieve their purposes.
- **Accuracy:** Personal data must be accurate and, where necessary, kept up to date.
- **Fair and lawful processing:** Organisations must process personal data fairly and lawfully, ensuring that they have a valid legal basis for collecting and using the data.
- **Storage limitation:** Personal data should not be kept for longer than necessary for the purposes for which it was collected.
- **Integrity and confidentiality:** Organisations must implement appropriate security measures to protect personal data.
- **Accountability:** Organisations are responsible for complying with data protection laws.

Cyber Essentials Scheme

Cyber Essentials is a cybersecurity certification scheme n the UK that outlines best practices for protecting against common cyber threats. The scheme encourages organisations to implement appropriate backup measures as part of their cybersecurity strategy. Under the Cyber Essentials framework, the following are essential:

Regular data backups

Secure storage

Sata retention policies

Frequent data testing

Data security policies and procedures

Data security policies and procedures are crucial for healthcare organisations in the UK to protect sensitive patient information and ensure compliance with relevant regulations.

While specific policies and procedures may vary based on the organisation's size and nature of operations, here are some common elements found in data security frameworks for healthcare organisations in the UK:

- **Data classification and handling:** Healthcare organisations classify data based on its sensitivity and establish guidelines for handling and protecting different categories of data.
- **Data retention and disposal:** Policies define retention periods for patient data and provide guidelines for secure data disposal once it is no longer required.
- **Access control:** Policies and procedures are in place to control access to patient information, ensuring that only authorised personnel can access and handle sensitive data.
- **Risk assessment and management:** Healthcare organisations perform regular assessments to identify potential vulnerabilities and implement controls to mitigate risks.

- **Staff training and awareness:** Regular training programs are conducted to educate staff about data security best practices, policies, and procedures, emphasising their role in safeguarding patient information.
- **Data encryption:** Encryption measures are implemented to protect data in transit and at rest, reducing the risk of unauthorised access or data breaches.
- **Incident response:** Procedures are established to detect, respond to, and manage data security incidents or breaches effectively, including reporting mechanisms and escalation procedures.

What problems data loss may cause for the healthcare industry?

The most common risks that arise from data loss within the healthcare industry include the following:

- **Compromised patient care:** Data loss disrupts access to critical patient information, impacting diagnosis, treatment plans, and care quality.
- **Loss of trust and reputation:** Data loss erodes patient trust, damaging the organisation's reputation and loyalty.
- **Financial implications:** Data loss incurs costs for data recovery, security improvements, and potential penalties for non-compliance.
- **Security and privacy risks:** Data loss exposes sensitive information, increasing the risk of fraud, identity theft, and privacy breaches.
- **Operational disruptions:** Data loss causes downtime, delays, and inefficiencies in healthcare operations.

Key Takeaway

Data backup is essential for your healthcare organisations to comply with regulations, protect patient information, and ensure uninterrupted operations.

Loss of data can compromise patient care, damage trust, result in financial implications, disrupt operations, and pose security risks. By implementing proper backup measures and adhering to data security policies, your organisation can mitigate these problems and maintain the integrity and privacy of sensitive healthcare data.

Make data compliance & protection simple with BackupVault

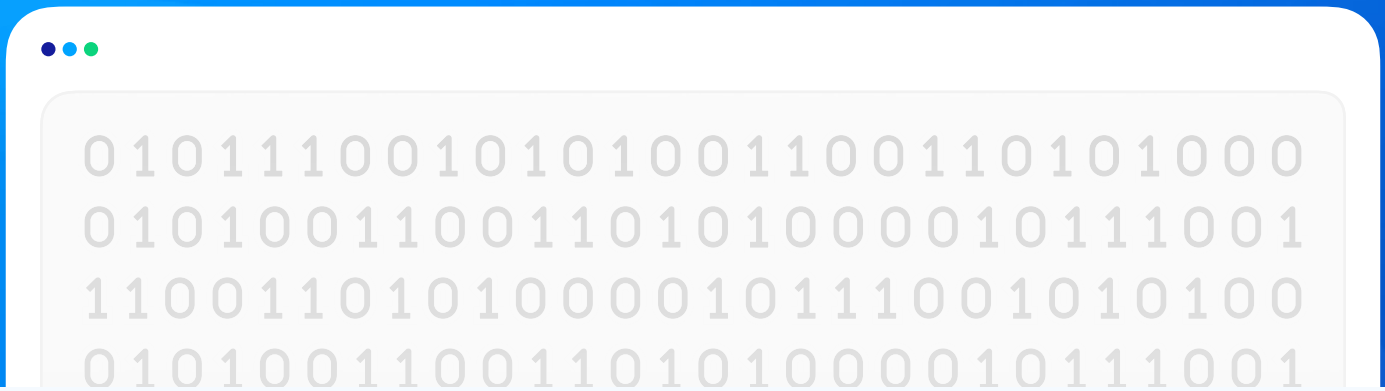
At BackupVault, we're dedicated to helping healthcare organisations achieve data compliance by providing robust backup solutions.

As data protection experts, we recognise the paramount importance of safeguarding your sensitive information from threats like ransomware, insider attacks, and hackers.

With our extensive expertise and access to multiple backup vendors, we offer independent advice to ensure you receive the ideal solution for your organisation.

We collaborate closely with you, assessing your specific requirements, and recommending the most suitable backup solution that aligns with your data protection goals.

Free trial



BACKUPVAULT

backup@backupvault.co.uk

020 3397 5159

Wilson House, Lorne Park Road
Bournemouth, Dorset, BH1 1JN