NODE4

Empowering business to do more

Managing Healthcare Data in an Era of Explosive Growth: A Guide to Storage Options

In partnership with

NetApp®

WPMHD21

Executive Summary

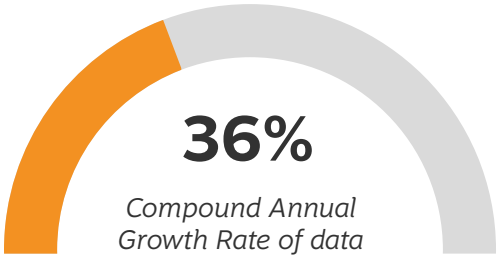
Electronic health records, high-resolution images, lab data, electronic prescriptions, health data from mobile and wearable devices, insurance information. These are just some of the fast-growing types of data that healthcare organisations and their suppliers must store securely, often for years at a time. And it's growing fast; an IDC report found that healthcare data is growing more quickly than any other business sector, at a compound annual growth rate (CAGR) of 36 per cent from 2018 to 2025.

> **"...an IDC report found that healthcare data is growing more quickly than any other business sector."**

All of this data must be stored in ways that make it accessible when needed, yet fully secure and in compliance with all regulations, in a cost-effective manner. Yet in many cases, healthcare organisations today have siloed pools of data stored in separate repositories, often in systems that don't scale well or don't have the security protections required today.

At a minimum, this mashup of approaches to storage can be ineffective, complex and expensive. At its worst, it could mean not being able to find documents required by auditors, the inability to glean insights from data, or even hackers finding ways to get to sensitive data.

In addition to the changes healthcare organisations are experiencing, the storage landscape has changed. Storage technologies have improved significantly, and the cloud is an unavoidable part of most storage scenarios. In short, there are more options than ever before, but the options are very good. It's just a matter of determining the best path forward for your organisation.



36%

Compound Annual Growth Rate of data within healthcare organisations, between 2018-2025

Modern Storage Technology: Focus on What's Important

> **Healthcare facilities need full, near-instant availability of data to make effective decisions and provide good patient care.**

Chances are, there was a time when the storage technology your healthcare organisation implemented was fast enough, and could easily meet storage requirements. Over time, as the technology ages and demands increase, storage technology often can't keep up. There comes a point for every healthcare organisation when it simply won't meet needs anymore, especially in these areas:

Availability and flexibility: More than ever, healthcare facilities need full, near-instant availability of data to make effective decisions and provide good patient care. At the same time, storage systems must be flexible enough to store data from a growing array of sources and adapt to changing requirements.

Scalability: Scalability is front-of-mind for many organisations experiencing significant data growth, especially in unstructured data like MRIs, CT scans, X-rays and PET scans. Storage systems must be scalable enough to continue meeting that demand. Keeping up with demand can mean buying much more infrastructure than required, just in case. For many organisations, the solution is moving at least some portion of storage resources to the cloud.

Latency: If it takes too much time to process a storage transaction or data request, the time lost is called latency. At best, slow data access is frustrating and impacts productivity. At worst, it can result in loss of life. Modern storage infrastructures are much more successful at reducing latency than legacy storage.

Case Studies

Challenge: A large healthcare provider with seven full-service hospitals and more than 60 clinics needed faster, high-performing storage to deliver critical data and applications to caregivers.

Solution: A series of all-flash storage arrays, which host the provider's Virtual Desktop Infrastructure (VDI) infrastructure as well as all on-premise servers and applications. The organisation now reports sub-millisecond response times, as well as significant data reduction through the deduplication and data compression features of the arrays.

Challenge: A large European healthcare organisation with more than 60 locations needed faster performance and a greater ability to scale.

Solution: A combination of high-performance NVMe running on flash arrays means caregivers can access clinical applications and data much more quickly.

Challenge: A large radiology provider with more than a dozen locations was growing rapidly. The provider stores nearly one million digital studies per year and adds about one million radiological images to its archive each year. In addition, the images are growing in size as well as volume.

Solution: A cloud-native global file system combined with Microsoft Azure object storage gives radiologist fast, local access to images through standard file-sharing protocols.

ROI: Getting the Most Value out of Your Storage Solution

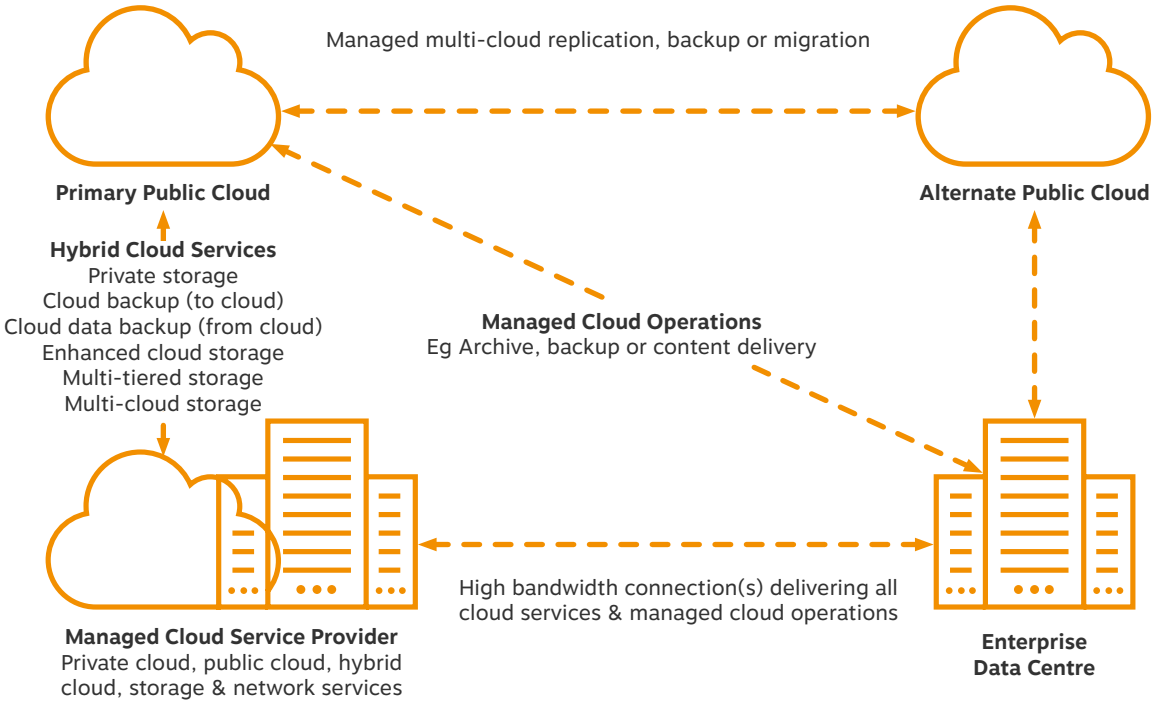
“Because organisations pay only for the capacity they use with cloud-based storage, costs can be lower.”

One of the most important decisions a healthcare organisation or supplier must make is whether it makes sense to move all applications and data to the cloud, or whether to choose a hybrid cloud infrastructure that keeps some workloads on-premises and moves others to the cloud.

Because security and privacy are always key issues for healthcare organisations, the temptation is to keep everything on-premises. While that can make sense for especially sensitive workloads and applications because it provides tighter controls, it may not be viable for the longer term, as the amount of data that must be managed and stored continues growing. On-premise storage environments, which require physical servers and other devices, are much less scalable than an elastic cloud environment. In many cases, this forces healthcare facilities to overbuy just to ensure enough space. In addition, those physical units require maintenance and upgrades over time, which can escalate costs and require additional on-site personnel.

Cloud-based storage, on the other hand, can scale as high as required. Cloud vendors also assure high availability and good performance. And because organisations pay only for the capacity they use with cloud-based storage, costs can be lower. The cloud model also allows healthcare organisations to store and access all data associated with a specific patient, procedure or business unit in one place.

Storage-Centric Managed Cloud Services (Service Models)



By its nature, data stored in the cloud promotes faster data exchange and sharing, which is becoming more important, especially in situations like the Covid-19 pandemic. In the UK, NHS Digital and the Private Healthcare Information Network (PHIN), in collaboration with the Department of Health and Social Care, NHS England, NHS Improvement and the Care Quality Commission (CQC), are working together to create a single source of healthcare data in England. This would not be possible without the cloud.

Cloud platforms also have come a long way when it comes to security, employing modern techniques like encryption and two-factor authentication. Yet for some workloads, this may not be enough.

That's why the majority of healthcare organisations and their suppliers choose the hybrid model, using the cloud for everything except the most sensitive data, which remains on-premises. Of course, that means choosing technologies and environments carefully and ensuring that facilities can seamlessly store and access data from both environments, as long as they have the right security credentials. Done right, this hybrid model protects data while improving access and cost.

Another increasingly popular option is to choose Storage as a Service (STaaS). With this model, an external provider owns and manages the storage infrastructure, while the healthcare facility can dictate storage, retention and access rules, along with service level requirements. This structure means that healthcare facilities can access storage on-demand, paying only for the amount they use, without worrying about buying, managing and maintaining physical devices. It also allows organisations to pay for storage via an OPEX model instead of typically more limited CAPEX funds.

Security, Compliance and Data Privacy

Protecting patient data is critical, not only to protect patients' privacy, but for the health of the healthcare organisation. Healthcare data breaches are notoriously expensive; one recent report put the average data breach cost at $7.13 million (£5.43 million). The report also noted that healthcare organisations take an average of 329 days to identify a violation—the highest of any industry.

Clearly, these numbers are unacceptable, and regulatory organisations around the world are doing what they can to turn the tide. National data privacy standards like Europe's General Data Protection Regulation (GDPR) and the United States' HIPAA can help. The GDPR, for example, outlines security and privacy regulations for all processing and data storage, including health information, related to people in the European Union. The regulation extends to any organisation that processes or stores data on these individuals.

While these regulations are a good first step in protecting and securing data, they can only go so far. The rest is up to organisations themselves. That means when it comes to storage, all data must be encrypted both in transit and at rest, and only the healthcare facility itself—not the provider—can control the keys. Data should also be transmitted as securely as possible, ideally over dedicated private lines.

But these are just table stakes. To remain fully secure, it's important to ensure that healthcare facilities' Chief Information Security Officers (CISO) have as much control and insight into the configuration, protection and destruction of data, even in a hybrid cloud model. In addition, it's important to ensure that every workload meets security requirements at every step along the way.

Data privacy and security go hand-in-hand with compliance. In the UK, for example, providers must adhere to GDPR. Healthcare organisations in England, Scotland and Wales must also adhere to security policies from the National Health Service (NHS), such as the Data Protection Act. The NHS' Department of Health and Social Care Information Center policy requires all organisations that process NHS patient data and

£5.43 million

is the average cost of a data breach

systems to provide assurances that they are practising good data security and that personal information is managed correctly.

These are complicated times for security and privacy. New threats occur almost daily, and new approaches to remaining secure also become available. Keeping on top of these trends is a full-time job. For some healthcare organisations, the choice to outsource that monitoring and protection is an easy one. If that's the case, look for a Security as a Service offering from an organisation that is extremely experienced in the healthcare arena and can provide the level of security and protection required.

Case Studies

Challenge: A data analytics supplier for the NHS wanted to adapt to the ever-evolving cyber security landscape and ensure their data remained as secure as possible.

Solution: They retained their virtual servers, but moved them behind fully managed Next Generation Firewalls, and implemented a VPN, providing their workforce with a single, secure route into them.

Challenge: A UK-based cosmetic surgery provider with more than 250,000 patients and 10TB of data was facing changes to its data retention requirements due to UK regulations.

Solution: By combining modern flash-based storage arrays, high-capacity disk drives, and an image-based replication solution, the organisation can easily meet industry regulatory requirements.

Challenge: A university hospital in Germany, which has been classified as an operator of critical infrastructure, must prove that its systems are fully protected against failures and cyber-attacks. In addition, the hospital must comply with legal storage regulations.

Solution: To address both challenges, the hospital first backs up all data to disk, and then again to tape. The availability strategy that entails storing data on different storage media also serves as a protection against ransomware attacks. The solution also generates evidence of compliance automatically.

Preparing for the Unexpected

> **Making sure current data is fully available at all times requires both a solid data backup and recovery solution, and a comprehensive disaster recovery plan.**

No matter how much effort healthcare facilities put into ensuring fast data access, accidents happen. Natural disasters, power outages and ransomware attacks are just some of the issues that can cause unintended downtime. It happens to every organisation; it's not a matter of if—it's just a matter of when. Yet immediate access to data is critical to both patient care and smoothly running healthcare facilities. Other impacts of lost data include loss of credibility and reputation, penalties for non-compliance with applicable data protection laws, and financial losses due to downtime and recovery costs, as well as potential litigation costs.

While choosing the right storage infrastructure is a critical part of ensuring that access, it's only one part. Making sure current data is fully available at all times requires both a solid data backup and recovery solution, and a comprehensive disaster recovery plan.

Data backup is the process of copying data to a separate location, and data recovery is the process of retrieving that backed up data so it can be restored and used. The typical rule of thumb is called the 3:2:1 rule: Have at least three different copies of data stored on two different types of media, with at least one of the backups stored offsite. Current data should be backed up several times per hour, and recovery should take only minutes.

There are plenty of technology choices when it comes to backup, from tape to the cloud. While tape may seem old-fashioned, it can be an ideal solution for long-term backup because it is relatively inexpensive, and it can be physically stored somewhere far from the facility. Cloud backups are more accessible and allow healthcare organisations to bring data and applications back online more quickly. When backing up in the cloud, consider an "air-gapped" approach, which protects data in case of a ransomware attack. Backups should be saved in the cloud as read-only and protected by two-factor authentication to safeguard against malware attacks.

To ensure that all data is fully protected, it's important to have a comprehensive disaster recovery/business continuity plan that is tested and updated regularly. The first step is assessing the risk of all assets, threats and vulnerabilities in the environment by conducting a business impact analysis. The analysis should also identify which systems, applications and data are most important to the organisation.

The next step in creating a good plan is developing a data backup plan, which should identify mission-critical applications and data along with the frequency of backups and retention. These are typically referred to as Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). RPO is the acceptable amount of time within which business functions or applications must be restored to acceptable levels of operational capacity. RTO is the maximum amount of time tolerable for data loss and capture.

The disaster recovery plan also should account for data protection laws, guidelines for how to keep running during outages, how to stay in touch with personnel, and directions for how to access data from disaster recovery locations.

While all of these steps are critical for every healthcare organisation, they also take a lot of care and feeding. For that reason, some healthcare organisations choose to use the managed services approach. Backup as a Service (BaaS), for example, enables healthcare organisations to do what they do best—provide patient care—while being confident that critical data is fully secure, backed up, available and in compliance with the organisation's rules. The same is true of Disaster Recovery as a Service (DRaaS), which can provide peace of mind by relying on an external provider to protect against disaster, based on the organisation's RPOs and RTOs.

Case Studies

Challenge: One of the largest healthcare facilities in Europe, with more than two dozen locations and more than one million patients per year, needed a way to ensure that data was available on demand.

Solution: The facility deployed backup of all data at all locations and replication to a remote location, where it is stored on disk and can be restored directly over the network if needed. With this solution, staff can back up, replicate and recover all virtual and physical workloads from a central management console.

Challenge: A rapidly growing European hospital found that its existing backup software could not keep up with the need to back up, store and protect growing volumes of data.

Solution: The storage environment is now centred around a Metro Storage cluster, which allows the application load to be flexibly distributed between two data centres. All productive data from virtual machines is stored on flash-based systems and mirrored between the two locations. Restores now take no longer than five minutes instead of hours.

Getting the most value from your data: The role of analytics

Increasing efficiency, improving patient outcomes and care quality, reducing costs—healthcare organisations are under pressure to achieve all of these and more. Although they might not seem related, data storage and access are important building blocks for achieving these goals. With the right tools, healthcare organisations can dive deeply into data, finding patterns, connecting the dots, and gaining important insights to support better decision-making.

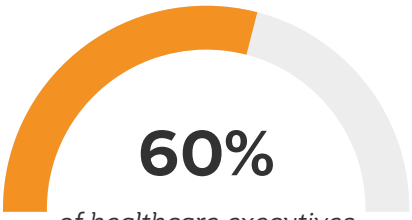
The possibilities are almost limitless. In general, however, there are two basic types of analytics: predictive analytics, which predicts what is most likely to happen; and prescriptive analytics, which identifies actions that can be taken to affect those outcomes.

Predictive analytics, which often employs technologies like statistical modelling, machine learning and artificial intelligence, uses historical data to predict future events. This method can be used to anticipate and reduce the risk of outcomes in many areas, from predicting the likelihood that a patient will experience complications after certain procedures to identifying when medical equipment might breakdown so service can be scheduled before that occurs.

These tools also can be applied to financial, administrative and data security challenges. In the security arena, predictive analytics can help identify security threats before they do damage.

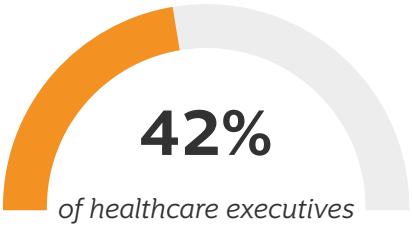
Because of its value, healthcare organisations are using predictive analytics in increasing numbers. According to one recent survey, 60 per cent of healthcare executives say their organisations are using predictive analytics. Of those, 42 per cent say patient satisfaction has improved, and 39 per cent have reduced costs.

Prescriptive analytics uses data modelling, data mining and artificial intelligence to analyse both historical and real-time data to "prescribe" possible actions and solutions for a problem. This method provides decision-makers with viable options and "what-if" scenarios. For example, suppose a walk-in clinic wants to design a facility with an optimum mix of services available to best meet patient needs. In that case, it could use prescriptive analytics to analyse a variety of important metrics. These could include the number of treatment rooms required for optimum efficiency, the most widely used clinic services, and other data points to determine the best design and optimal staff mix.



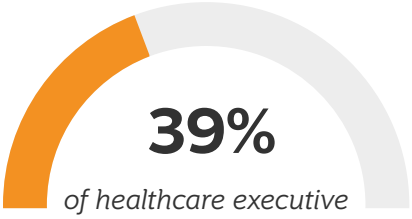
60%

of healthcare executives say their organisations are using predictive analytics.



42%

of healthcare executives say patient satisfaction has improved as a result of predictive analytics.



39%

of healthcare executive have reduced costs by using predictive analytics.

“With the right tools, healthcare organisations can dive deeply into data, finding patterns, connecting the dots, and gaining important insights to support better decision-making.”

Case Studies

Challenge: A German medical school needed a better way to efficiently analyse large quantities of data, including images and lab results. Existing methods took as long as a day to analyse a single case, and required technicians to manually transform image data into clinically relevant information.

Solution: Using a data infrastructure that can handle massive data sets along with big data diagnostics and analytics tools, researchers were able to run five times as much data simultaneously. This resulted in much faster diagnoses.

Challenge: A regional hospital needed to find a way to better analyse hospital infections, improve physician performance and identify treatment trends.

Solution: The hospital implemented an analytics platform that allows them to glean more insights from both historical and real-time data through interactive, intuitive visual analysis. For example, the hospital’s endoscopy unit now saves about 15 hours each week by automating analysis instead of generating manual reports on procedures performed. Automated analysis also has enabled the hospital to better analyse costs and success rates associated with individual providers.

The Crisis Test: Will Your Data Infrastructure Measure up During Times of Crisis?

There is nothing like a crisis to put an organisation's data storage and infrastructure to the test. The Covid-19 pandemic, for example, has stretched capacity, functionality and security to the brink for hospitals, healthcare suppliers, labs and even government-sponsored universal healthcare systems. That's because in times of crisis, there is typically a lot of new data to store, manage, secure and analyse, and it must be accessible in new ways.

For example, telehealth has skyrocketed. In the United States, healthcare providers are seeing as many as 175 times the number of patients via telehealth than before COVID-19. In Europe, telemedicine has grown significantly, and 73 per cent of medical specialists say they will continue to use telemedicine after the current crisis is over. While telehealth helps keep citizens healthy without unduly exposing them to other health threats, it also requires more devices and connections, and sometimes, transfers of data in new ways.

Data sharing also increases during crises, both to collaborate on solutions and triage and diagnose patients. This requires a lot in terms of data performance, accessibility and security. For example, soon after it became clear that COVID-19 was an international pandemic, the UK's National Health Service partnered with Google, Microsoft and other tech organisations. They quickly got to work developing a data storage system that would combine data sources from NHS and social care organisations to help support the country's response to COVID-19.

Crises also tend to bring out the opportunists, in the form of higher rates of ransomware, phishing and other cybersecurity attacks. Healthcare organisations also tend to relax security requirements during times of crisis to meet physician needs and facilitate telehealth, which just makes it easier for hackers to access private data. Strong storage security is essential.

“In times of crisis, there is typically a lot of new data to store, manage, secure and analyse....”

All of these factors have put storage capacity, management and security to the test. Few pass with flying colours, and in many cases, it is serving as a wake-up call. For organisations that have not yet fully embraced the cloud, the current crisis may provide the push they need. With the cloud model, healthcare organisations can expand data stores without hitting the ceiling, while taking advantage of the security features that cloud storage can provide. The cloud also provides a valuable platform for data sharing and accessibility, and can accommodate the needs of healthcare employees working remotely.

The pandemic also has demonstrated the importance of being able to analyse comprehensive data stores. A cloud data lake, for example—a central repository for storing structured and unstructured data—can give healthcare organisations the consolidated data they need to quickly analyse data sets. For example, a hospital could use that data to predict ER overcrowding or patient surges.

There is at least one positive outcome from a health crisis. Healthcare organisations that use that crisis as a spur to improving data management, performance, accessibility and usability will be better prepared for whatever comes next.

Conclusion: Looking Forward

The rules surrounding the security, privacy and retention requirements of healthcare data continue to change, and the storage infrastructure you choose has to keep up. For example, the European Commission is calling for the creation of the Common European Health Data Space, designed to promote better exchange and access to different types of health data. The Global Consortium for eHealth Interoperability is another group with big changes in mind. Its goal is to enable healthcare systems and governments to agree on interoperability standards for secure data access. Whatever form these initiatives take, they are likely to require some changes in the way healthcare organisations and their suppliers store, protect and share data.

There's also the completion of the Brexit process in January 2021 to consider. It's shown that the stability of political and legal frameworks is no longer a given. Organisations must review the location of critical data such as lifetime medical records. De-staging of certain types of data from the cloud is one viable option, and independent onshore cloud providers are perfectly placed to assist here.

In addition to keeping pace with changing regulations and requirements, healthcare organisations also must be able to incorporate emerging technologies and new kinds of data without "ripping and replacing" its entire storage infrastructure. For example, new types of data will have to be stored securely—data from streaming telehealth sessions, new types of Internet of Things (IoT) devices, and consumer health devices.

Telehealth is destined to grow; while it got a big push from the Coronavirus pandemic, new 5G connectivity, with its improved speed and lower latency, will become more important to healthcare. Better connectivity also will boost the use of augmented reality, not only for telemedicine but in other areas of healthcare.

That's just the tip of the iceberg. Other trends, such as the move toward greater personalisation in healthcare, the use of blockchain and quantum computing, and the burgeoning use of artificial intelligence and machine learning, will create ever-larger data sets.

The potential for technology to improve healthcare is almost limitless. The key is remembering where it starts and ends—with data.

Node4's Approach to Data Storage

Since our inception in 2004, we have focused on providing data-focused solutions that solve big problems for our customers. To ensure the highest quality, we combine top technology from leaders like NetApp, Red Hat, Oracle, Veeam and Zerto with expertise in IT infrastructure services and hybrid, private and public cloud. Our managed services approach to data services ensures attention to detail, flexibility and the highest levels of customer service.

We have helped solve data storage and management challenges for some of the most prestigious healthcare organisations and suppliers in the UK. For BMI Healthcare, a large healthcare organisation with 58 outposts throughout the UK, we implemented a new WAN solution and consolidated hosting gateways for both servers and storage. Today, BMI Healthcare uses those gateways to access other cloud services, all delivered by Node4 as a managed service. For Benenden Health, we replaced an ageing infrastructure with a hybrid cloud and disaster recovery solution. The new cloud-first, DR-supported architecture helps Benenden Health keep sensitive data secure and provides a path for the organisation to adopt more cloud-based technologies.

Beyond data services, we offer a broad portfolio of solutions, including cloud services to support hybrid and multi-cloud models, HSCN connectivity, collaboration and security. This enables us to think outside of the box when it comes to understanding your business requirements, and engineer the right solution for you.

Our managed data services

Storage as a Service
Access to a variety of cloud providers, while keeping data secure in one of Node4's data centres.

Backup as a Service
Backup solutions through cloud and physical devices, including backup of Office 365 content.

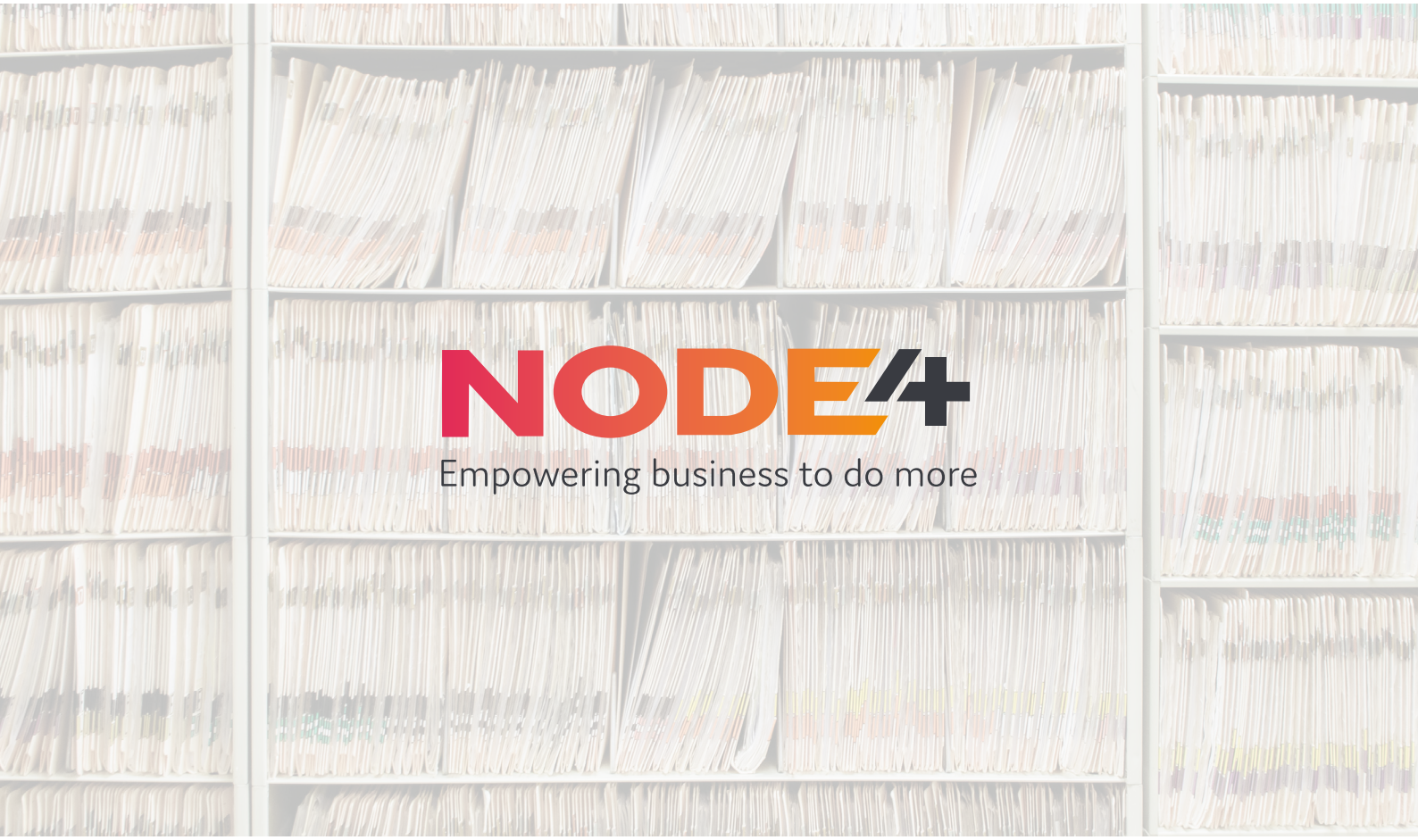
Disaster Recovery as a Service
Protection between N4 Cloud data centres or your premises and the N4 Cloud.

Managed Backup from Cloud
Backup or de-stage critical data from public cloud to an independent service or on-premises repository.

Get in touch

Our expert team look forward to hearing from you and seeing how we can empower your organisation to do more:

Call: 0845 1232222
Email: sales@node4.co.uk
Website: node4.co.uk/contact



WPMHD21

Node4 Ltd Registered in England No. 04759927 VAT: 192 2491 01
Registered Address: Millennium Way, Pride Park, Derby DE24 8HZ
T: 0345123 2222 **E:** info@node4.co.uk
www.node4.co.uk