WHITE PAPER

Cyber protection solutions for 21st-century healthcare industry challenges

How healthcare tech professionals can protect sensitive data in the new era of cyberthreats.

The healthcare industry is undergoing a pivotal digital transformation, moving from antiquated methods of storing patient information to adopting new data-intensive diagnostic and treatment applications. At the same time, healthcare institutions face enormous pressure to grow profits, comply with privacy regulations, optimize patient care, and improve interoperability with payers, suppliers, delivery partners, academic institutions, and patients.

The sheer volume of sensitive healthcare data is growing and spreading across physical locations, computing devices, and networks (including private and public clouds). Important new healthcare applications like telemedicine, remote patient monitoring, and virtual- and assisted-reality-based training are adding to the flood of data. Other emerging technologies like artificial intelligence (AI), machine learning (ML), the Internet of Things (IoT), and blockchain further complicate the puzzle – all as more users clamor to access that data.

Meanwhile, the industry is besieged by a flood of new cyberthreats, including privacy breaches, ransomware attacks, and cryptojacking campaigns. It has never been a more complex time to try to maintain the availability, accessibility, and privacy of healthcare data.

Cybercriminals and hostile state actors have aggressively targeted the healthcare industry, exploiting the fact that malware attacks like ransomware are especially effective when access to sensitive data is a matter of life and death.

This explains the rash of high-profile ransomware attacks on hospitals in recent years, including the National Health Service in the UK, Hancock Health, Adams Memorial Hospital, MedStar Health, Erie County Medical, and many others. Data breaches in the sector are a regular news item, with hundreds of millions of sensitive patient records and payment records stolen every year.

The industry also sits in the crosshairs of compliance authorities focused on privacy regulations including the USA's Health Insurance Portability and Accountability Act (HIPAA), the European Union's General Data Protection Regulation (GDPR), and state-level privacy regulations in the USA such as the California Consumer Privacy Act (CCPA). Industry players are also at risk of violating credit-card regulatory standards like the Payment Card Industry Data Security Standard (PCI DSS).

The growing reliance on electronic patient data has further heightened the importance of non-stop availability. In addition to the obvious threat to patient safety that downtime represents, it can be costly enough to pose an existential threat to the viability of healthcare institutions. According to Gartner's "Downtime Cost Calculator for Data Center Disaster Recovery Planning, 28 February 2014", the average cost of downtime for all types of businesses is $5,600 per minute, or roughly $300,000 per hour. Information Technology Intelligence Consulting concludes that **for 98% of businesses, a single hour of downtime costs more than $100,000, and as much as $1M to $5M for many larger businesses.**

Survival in the face of these challenges requires a new approach to safeguarding data that is built on the Five Vectors of Cyber Protection:

SAFETY
Ensuring that a reliable copy of data is always available

ACCESSIBILITY
Making data easily available from anywhere at any time

PRIVACY
Controlling who has visibility and access to your data

AUTHENTICITY
Creating undeniable proof that copies of data exactly replicate the originals

SECURITY
Protecting data, applications, and systems from malicious threats

Meanwhile, IT departments at healthcare institutions suffer the same challenges that afflict all industries: growing infrastructure complexity, the difficulty of recruiting and retaining skilled staff, the ongoing migration of applications to private and public clouds, the proliferation of mobile devices like smartphones and tablets, the advent of IoT sensors, asset trackers, and web cameras, and the need to conduct near-real-time analytics on new data.

This paper examines these fundamental cyberprotection principles in the face of seven key challenges to the healthcare industry:

1. **Addressing** data breaches
2. **Protecting** against malware threats like ransomware and cryptojacking
3. **Meeting** compliance requirements
4. **Migrating** critical applications and storage to public and private clouds
5. **Delivering** constant data availability
6. **Incorporating** mobile devices
7. **Strengthening** data protection without adding infrastructure complexity

THE STATE OF HEALTHCARE IT

Data protection and security remain a top priority for today's healthcare organizations. In its study of data breaches, the cybersecurity firm Protenus found that the pace of healthcare industry attacks was more than one breach per day in 2017.

The same year, 5.6 million patient records were breached and it took an average of 308 days for an institution to even discover that a breach had occurred.

Curtailing the number of healthcare data breaches requires layers of IT infrastructure security around physical systems, virtual machines (VMs), cloud services, and mobile devices. Basic countermeasures include anti-malware protection on endpoints, defenses against external network threats using firewalls, and network segmentation via vLANs or software-defined networking to limit the propagation of attacks across internal networks. Data protection in the form of backup and disaster recovery is essential in the event that an attack damages, destroys, or denies access to sensitive data. This requires secure, ideally encrypted backup and storage both on premises and in the cloud.

MALWARE THREATS

According to most security researchers, the two most pervasive malware threats in recent years to afflict the healthcare industry are ransomware and cryptojacking.

Ransomware infects healthcare servers, desktops, and mobile devices (usually by a user clicking on a malicious link or attachment in a phishing email), encrypts any data it finds, and then demands an online payment for the decryption key necessary to unlock the victim's files. Without countermeasures to detect and terminate ransomware attacks, or the ability to restore from a recent backup, many healthcare institutions have suffered downtime that has threatened patients' lives and cost millions of dollars in lost productivity and remediation costs.

Cryptojacking is a less overt but growing type of cyberattack in which infected healthcare machines become zombies in botnets that mine cryptocurrency on behalf of cybercriminals. The malware only steals resources from its victims – computing cycles, memory, electricity, and cooling – but the resulting energy costs and wear and tear on systems add up. In addition, cryptomining malware often injects other threats such as ransomware into the system it infects.

COMPLIANCE REQUIREMENTS

Regulatory scrutiny of the healthcare industry has helped make it a favorite target of cybercriminals wielding malware like ransomware. The risk of compliance violations caused by sensitive patient data being locked up by a ransomware attack makes victims likelier to promptly pay the extortion in order to regain access to the data.

For the second straight year, ransomware attacks accounted for **over 70% of all malware incidents in the healthcare sector,** according to the "2019 Verizon Breach Investigations Report."

APPLICATION AND STORAGE MIGRATION CLOUD

Like most industries, healthcare is in the middle of a long journey to migrate its core applications and data to a mix of public and private cloud infrastructure. The goal is to cut costs, trade depreciating capital assets for predictable service costs, and improve data accessibility and sharing from any location or device. However, many institutions struggle with the challenges of safely moving storage and data protection resources to the cloud while maintaining data privacy and regulatory compliance.

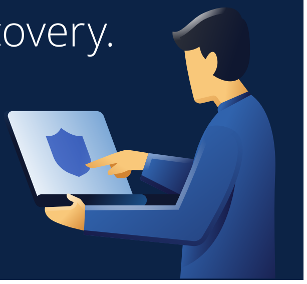
For the second straight year, ransomware attacks accounted for over 70% of all malware incidents in the healthcare sector, according to the "2019 Verizon Breach Investigations Report."

DATA AVAILABILITY

The healthcare industry has obvious reasons to value high and continuous data availability: patient health and survival often depend on it.

From a backup and recovery perspective, this requires that healthcare IT professionals pay close attention to two metrics: the Recovery Point Objective (RPO) and Restore Time Objective (RTO). RPO defines how much information an institution can afford to lose at any given moment: in effect, how frequently it needs to create backups of its critical data. RTO reflects the amount of downtime an institution can endure between the time of a data failure event and successful recovery from it. Most institutions can easily identify which applications require more stringent RPOs and RTOs, and which ones can abide greater data loss and longer recovery times.

> Acronis offers healthcare institutions a complete set of easy-to-use, extremely flexible and tightly-integrated solutions for cyber protection, storage, and disaster recovery.



BYOD RISKS

The advent of ubiquitous employee-owned devices in healthcare has reaped several benefits to the industry, including improved staff productivity and collaboration. But it also presents data protection challenges as sensitive data is now likelier to be stored on devices that are easily compromised, lost, or stolen.

SIMPLIFIED CYBER PROTECTION

As in many industries, healthcare IT managers are struggling to staff their operations with skilled professionals, so eliminating operational complexity has become a top priority. This is particularly important for routine operational issues like data protection. Deploying multiple systems to manage a diverse IT environment and requiring highly-skilled engineers to run it, is sub-optimal.

HOW ACRONIS DELIVERS CYBER PROTECTION SOLUTIONS FOR HEALTHCARE

Acronis provides protection against data breaches in several ways. Acronis Cyber Backup provides encryption of sensitive data in transit and at rest to ensure that even in the event of a successful data breach, cybercriminals cannot benefit from the information they have compromised.

Acronis Cyber Backup also provides the ability to completely restore data that has been tampered with, destroyed, or locked up by a cyberattack.

Acronis Cyber Cloud Storage protects data and backups from breaches with a formidable array of cyber defenses, including strong encryption of data and backups (both in transit and at rest) and certified, secure cloud data centers.

PROTECTING AGAINST MALWARE THREATS LIKE RANSOMWARE AND CRYPTOJACKING

Acronis Cyber Backup with Acronis Active Protection uses AI and ML to actively detect, block, and reverse suspicious changes to data, backup files, and backup agents – reverting file changes using the cache. It also automatically detects and terminates cryptojacking attacks.

This provides an unparalleled defense against two of the most pervasive malware threats to the healthcare industry, adding zero-day threat defenses to complement legacy countermeasures like signature-based anti-virus software.

Acronis Cyber Backup also hardens its backup agent and archives against malware attacks, ensuring that a breach cannot compromise the institution's ability to recover swiftly and resume normal operations after a breach.

MEETING COMPLIANCE REQUIREMENTS

The encryption capabilities of Acronis Cyber Backup with Acronis Active Protection and Acronis Cyber Cloud Storage also support compliance goals by protecting the privacy of sensitive healthcare information – rendering it useless to cybercriminals even in the event of a successful breach. Acronis products have many other native functions and features that, when configured and used properly, support compliance with applicable parts of HIPAA as well as the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). While there is no official, legally recognized certification process or accreditation for HIPAA or HITECH, **Acronis maintains a security and compliance program designed to minimize customer HIPAA and HITECH compliance concerns.** For more information, visit the Acronis Resource Center.

MIGRATING CRITICAL APPLICATIONS AND STORAGE TO PUBLIC AND PRIVATE CLOUDS

Acronis Cyber Backup simplifies the process of migrating healthcare applications to the cloud by supporting a broad range of cloud services, operating systems (physical and virtual), application workloads (both premise- and cloud-based), and endpoints. Acronis Cyber Backup's array of data management tools make it simple and safe to move workloads between physical, virtual, and cloud environments to enable fast, risk-free migration to new platforms, including private clouds, Acronis Cyber Cloud Storage, and popular public-cloud offerings from Amazon, Google, and Microsoft.

DELIVERING CONSTANT DATA AVAILABILITY

Acronis Cyber Backup provides useful features to help healthcare institutions intelligently manage RTOs and RPOs across their application environment, including:

1. Acronis Instant Restore, which delivers near-zero RTOs and RPOs for the most critical applications
2. Acronis Universal Restore, which provides great flexibility to restore a system to new bare-metal hardware or a different platform, e.g., from a physical to a virtual machine when necessary
3. Built-in Acronis Active Protection, which eliminates the downtime and performance degradation associated with ransomware and cryptojacking attacks.

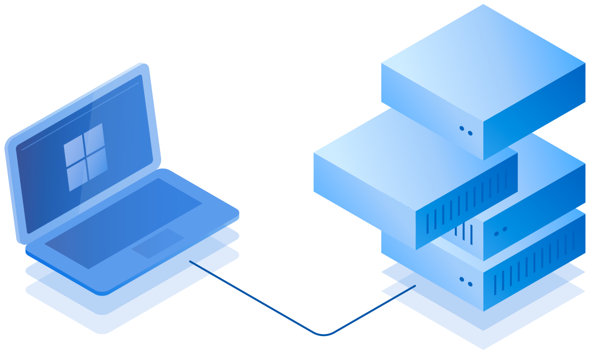
PROTECTING SENSITIVE DATA ACROSS ALL DEVICES

Acronis Files Advanced helps to enhance patient care and improve operational efficiency, while ensuring adherence to strict security and compliance standards, including the Health Insurance Portability and Accountability Act (HIPAA). Using Acronis Files Advanced, healthcare employees, partners, and contractors can share and collaborate on sensitive documents. Meanwhile, institutions retain complete control over data location, management, and privacy.

The Acronis Files Advanced policy engine provides granular management capabilities to ensure control and compliance for content, users, and devices. The solution also guarantees complete data protection and confidentiality via secure end-to-end encryption of data at rest and in-transit. In addition, Acronis Files Advanced enables IT to prevent information leaks, data sharing violations, and security breaches via centralized policy controls.

Healthcare providers, practices, and patients use Acronis Files Advanced to access, edit, create, and share healthcare data across any device – desktop, laptop, tablet, or smartphone. In addition, healthcare practices leverage the solution to:

- **Protect** both sensitive patient data and administrative documents (e.g. confidential information and research, academic and corporate contracts, etc.)
- **Give** doctors, researchers, and medical administrators secure access to healthcare data and enable easy sharing from any device
- **Secure** patients' records both at rest and in-transit
- **Collaborate** quickly and efficiently on patient care, both internally (within the healthcare organization) and externally (with partners)
- **Track** healthcare file access and sharing
- **Meet** strict security and compliance standards, including HIPAA



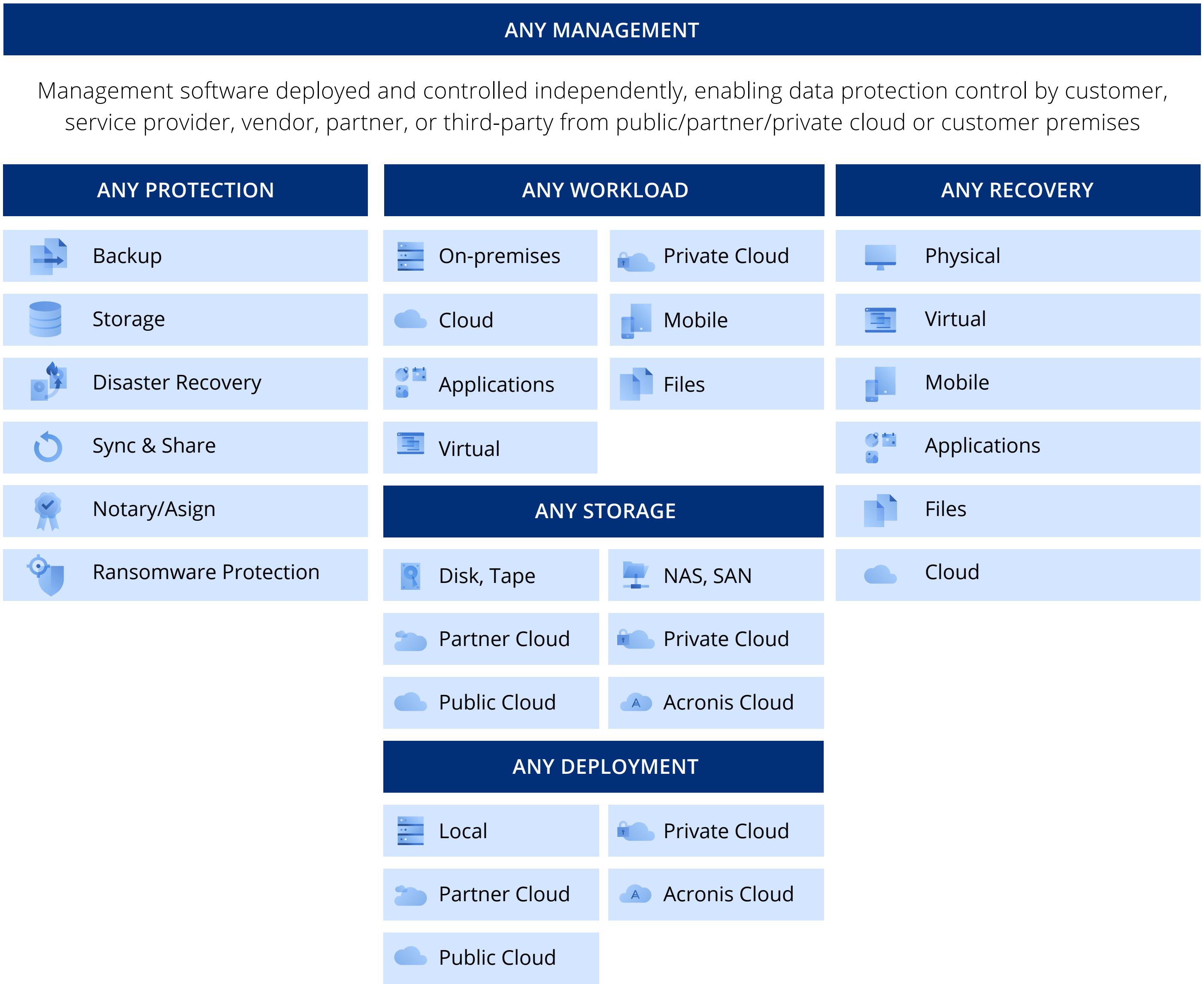
STRENGTHENING CYBER PROTECTION WITHOUT ADDING INFRASTRUCTURE COMPLEXITY

Acronis Cyber Backup simplifies and lowers the cost of healthcare cyber protection operations by providing a single platform that can protect all of an institution's workloads.

It can manage storage, retention, backups, and recovery operations across the board, including cloud, virtual, physical, and mobile platforms as well as popular workloads from Microsoft, Oracle, Google, and others. Furthermore, the powerful and intuitive interface and monitoring tools make it easy enough for relatively junior IT staffers to run it, allowing more experienced staffers to focus on more strategic projects.

Finally, the Acronis Disaster Recovery Add-On is a simple, easy-to-use extension to Acronis Cyber Backup. It enables healthcare institutions to instantly recover from the failure of critical IT systems, applications, and data by automatically switching over to backups running on virtual machines running in the secure Acronis Cloud. It provides failover for a wide variety of popular computing platforms and applications, including Windows Server, Linux, virtualization platforms including VMware, Hyper-V, KVM, XenServer, and Red Hat Virtualization, and Microsoft applications including Exchange, SQL Server, SharePoint, and Active Directory.

ACRONIS' UNIQUE CLOUD ARCHITECTURE GIVES YOU CONTROL OVER YOUR DATA



ANY MANAGEMENT

Management software deployed and controlled independently, enabling data protection control by customer, service provider, vendor, partner, or third-party from public/partner/private cloud or customer premises

ANY PROTECTION

- Backup
- Storage
- Disaster Recovery
- Sync & Share
- Notary/Asign
- Ransomware Protection

ANY WORKLOAD

- On-premises
- Private Cloud
- Cloud
- Mobile
- Applications
- Files
- Virtual

ANY STORAGE

- Disk, Tape
- NAS, SAN
- Partner Cloud
- Private Cloud
- Public Cloud
- Acronis Cloud

ANY DEPLOYMENT

- Local
- Private Cloud
- Partner Cloud
- Acronis Cloud
- Public Cloud

ANY RECOVERY

- Physical
- Virtual
- Mobile
- Applications
- Files
- Cloud

CONCLUSION

The combination of rapid digital transformation, surging data volumes, growing interoperability needs, and increased scrutiny from shareholders and regulators make this a challenging time for the healthcare industry. Balancing the simultaneous delivery of data safety, accessibility, privacy, authenticity, and security is a delicate one, especially when facing off armies of cybercriminals determined to steal valuable healthcare data and hold it for ransom. Healthcare institutions are expected to enable complex new applications, drive down costs, and improve patient outcomes – all while fighting off broad IT challenges like staff retention, cloud migration, and the proliferation of mobile and IoT devices.

Acronis can help with a proven array of cyber protection, storage, secure file sync-and-share, and disaster recovery solutions that are optimized for the healthcare industry.

See how Acronis cyber protection solutions have already benefited a US hospital here.

Get a complimentary **30-day trial of Acronis products** for healthcare here:

- Acronis Cyber Backup with Acronis Active Protection GET A 30-DAY FREE TRIAL
- Acronis Disaster Recovery Add-On for Acronis Cyber Backup GET A 30-DAY FREE TRIAL
- Acronis Files Advanced GET A 30-DAY FREE TRIAL

Acronis

Learn more at
www.acronis.com