

Data Protection & Security in Healthcare

Challenges and a Smarter Path Forward

Healthcare organizations are operating in an increasingly complex environment. Rising costs, staffing shortages, evolving regulations, and rapid digital transformation are forcing IT leaders to rethink how infrastructure and security are approached.

At the same time, cyber threats are increasing in both frequency and scale. For healthcare organizations, the impact of a security incident extends far beyond financial loss. It affects operations, compliance, and most importantly, patient care.

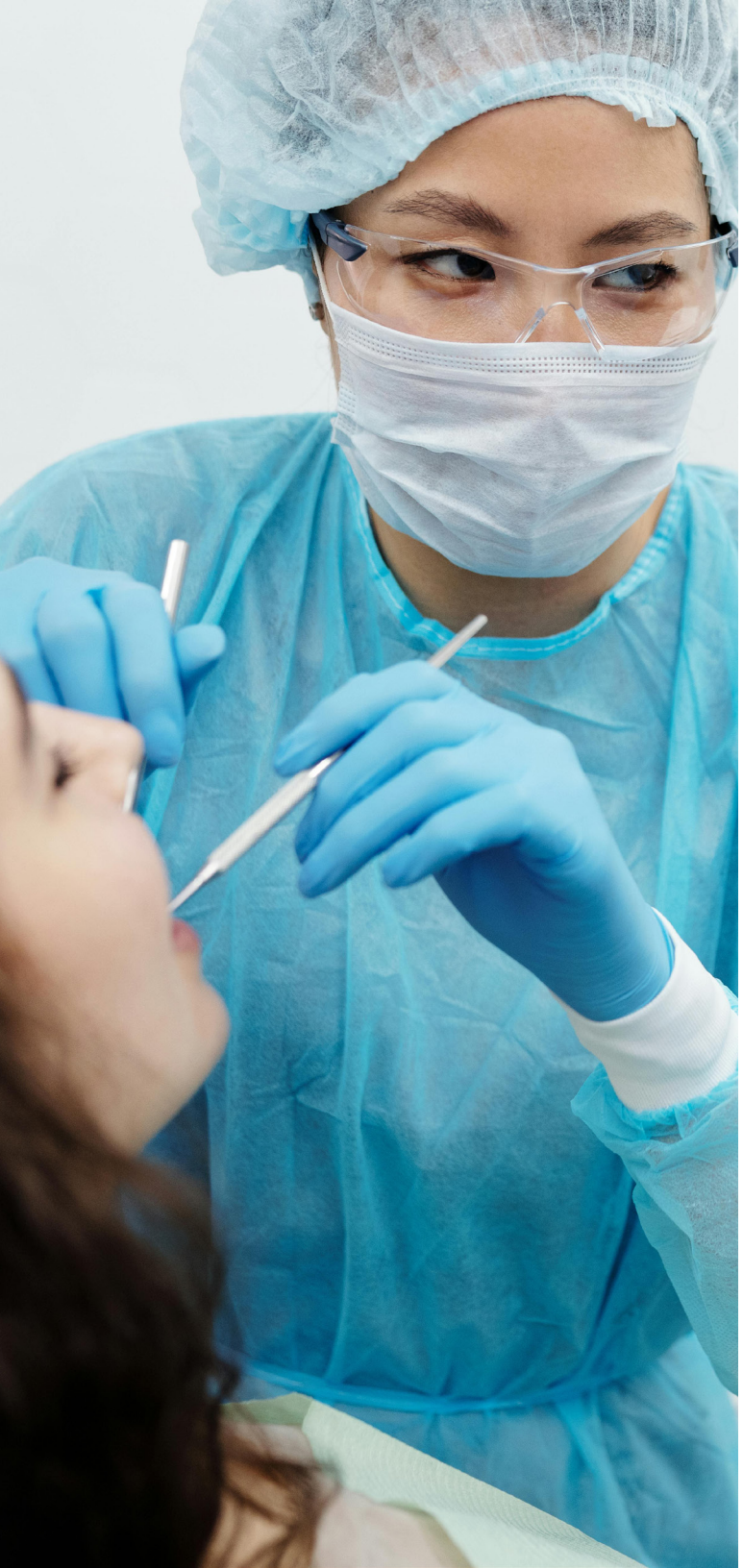
Data protection is no longer just an IT concern. It is a foundational part of how healthcare organizations operate.

The State of Healthcare Security

- *60+ major healthcare breaches per month in 2025*
- *Millions of patient records exposed in single incidents*
- *Healthcare remains a top target for ransomware*

Sources: HIPAA Journal, Cobalt, Reuters (2025)





An Industry at Risk

The healthcare sector remains one of the most targeted industries for cyberattacks, but the nature of these attacks is shifting. Rather than isolated incidents, organizations are now facing larger, more coordinated events that impact entire systems of care.

In 2025, **healthcare organizations experienced more than 60 major breaches per month on average**, with some of the largest incidents affecting millions of individuals in a single event. These large-scale breaches are often tied to third-party systems, shared platforms, or widely used technologies, increasing the downstream impact across multiple organizations.

As healthcare environments become more connected, risk is no longer contained. It moves across providers, partners, and platforms, making resilience just as important as prevention.



The High Value of Healthcare Data

Healthcare data continues to be one of the most valuable assets targeted by cybercriminals. Protected Health Information includes deeply personal identifiers such as Social Security numbers, medical histories, and insurance details. Unlike financial data, which can often be reset, this information remains valuable over time.

This persistence is what makes healthcare data particularly attractive. Once exposed, it can be used for identity theft, insurance fraud, and targeted attacks long after the initial breach occurs. It also means that the impact of a breach is not short-lived.



The True Cost of a Breach

The cost of a healthcare data breach continues to outpace every other industry. **Recent reports place the average cost at approximately $7.4 million, with some incidents exceeding $10 million when long-term impacts are included.**

These costs are driven by more than just remediation. Organizations must manage operational disruption, regulatory exposure, and the loss of patient trust, all while continuing to deliver care.

Healthcare breaches also take significantly longer to identify and contain than in other industries, often approaching nine months. During that time, systems remain vulnerable and data may continue to be exposed.

The Cost of a Breach

- *Average healthcare breach cost: ~$7.4 million*
- *Some breaches exceed $10 million*
- *Average time to identify and contain: ~279 days*

Sources: IBM Cost of a Data Breach Report; Baker Donelson (2025)



No Time for Downtime

In healthcare, downtime is not just a technical issue. It is a direct risk to patient care.

When systems become unavailable, clinicians lose access to critical tools such as electronic health records, imaging systems, and clinical applications. This can delay treatment, disrupt workflows, and increase the likelihood of errors.

Recent cyber incidents have shown how quickly downtime can cascade. What begins as a security event can evolve into a broader operational disruption affecting scheduling, communications, and administrative systems.



Where the Risks Are

The healthcare threat landscape has expanded alongside digital transformation. Ransomware remains one of the most visible threats, often targeting healthcare organizations because of the urgency to restore operations. At the same time, identity-based attacks, including phishing and credential misuse, have become increasingly common and difficult to detect.

The growth of connected devices has introduced additional complexity. Medical devices and IoT systems expand the attack surface, often without consistent security controls or visibility. Emerging technologies such as AI are adding new considerations around data access, governance, and risk.

Most risks in healthcare environments fall into a few key categories:

- External attacks such as ransomware and malware
- Credential-based access through phishing or misuse
- Expanding attack surfaces from connected devices
- Internal risks driven by misconfiguration or human error



The Reality of Human Error & Insider Risk

Not all threats originate outside the organization. In healthcare, many incidents can be traced back to internal factors, often unintentional.

Employees may access data from unsecured devices, fall victim to phishing attempts, or bypass protocols to complete tasks more quickly. In other cases, excessive access privileges or poor system configuration can create exposure without anyone realizing it.

These types of incidents are particularly challenging because they involve legitimate access, making them harder to detect and often slower to resolve.

Where Most Risk Starts

Most healthcare security incidents can be traced to:

- *Human error or negligence*
- *Credential compromise*
- *Misconfigured systems*
- *Lack of visibility across environments*

Security must address both technology and behavior.



Making Security a Business Imperative

For many organizations, security has historically been approached as a cost decision. Investments were often weighed against immediate budget pressures rather than long-term risk.

That approach is no longer sustainable.

The cost of a breach now extends far beyond the initial incident. Recovery efforts, compliance remediation, and operational disruption can have lasting impacts. As a result, more organizations are treating security as a core business function rather than a supporting role.

Security is no longer just about prevention. It is about ensuring the organization can continue to operate under any conditions.



Building a Practical Security Strategy

An effective data protection strategy begins with understanding the data itself. Organizations must have clear visibility into where data resides, how it moves, and who has access to it.

From there, security should be aligned to the way data flows through the organization. This includes protecting endpoints, securing applications, monitoring networks, and ensuring cloud environments are properly configured.

Strong strategies consistently include:

- Clear visibility into data and access
- Security controls aligned to usage and movement
- A tested incident response plan
- Ongoing compliance alignment
- Defined policies for remote access
- Reliable backup and recovery capabilities



Prioritizing Disaster Recovery

In healthcare, protecting data is only part of the equation. Organizations must also be able to recover it quickly and reliably.

Downtime can disrupt care delivery, delay critical decisions, and create compliance challenges. Because of this, disaster recovery planning must go beyond simple backup strategies.

A strong approach ensures that data is not only preserved, but accessible when needed. This includes defined recovery objectives, failover capabilities, and regular testing.

Disaster Recovery Essentials

- *Secure, regular backups*
- *Defined RTOs and RPOs*
- *Failover to alternate environments*
- *Ongoing recovery testing*

Reliance must be proven, not assumed.



The Right Tools. The Right Partner.

Healthcare IT environments are complex, and there is no single solution that addresses every challenge. Each organization has its own mix of systems, applications, and operational requirements.

What matters is having the right combination of technology and expertise.

US Signal works with healthcare organizations to design solutions that support security, compliance, and long-term flexibility. By combining cloud infrastructure, data protection, and managed security services, organizations can modernize without disruption.

Run Healthcare IT Smarter

Healthcare IT leaders are being asked to balance cost, performance, and risk in ways that were not required just a few years ago. The organizations that succeed will take a proactive approach. They will invest in resilience, align security with business priorities, and build infrastructure that can adapt as needs evolve.

Because in healthcare, the stakes are higher than in any other industry.
Protecting data is essential.

But protecting patient care is what matters most.

