

Healthcare Data Security: 5 Best Practices for Modern Medical Practices



Healthcare organizations continue to be a top target for cybercriminals. In 2025, around 379,306 individuals daily had their personal and protected health information breached. At the same time, healthcare continues to hold the highest average cost of a data breach among industries for the 14th year in a row.

As these threats escalate, it's clear that medical practices need a proactive, multi-step approach to data security that safeguards patient information, supports compliance, and strengthens operational resilience.

1. Build a Strong Security and Compliance Foundation

A strong security foundation starts with treating HIPAA compliance as an ongoing process. Regular risk assessments, security audits, and continuous monitoring of systems handling protected health information can help practices identify vulnerabilities and strengthen safeguards before issues arise. Consider designating a security leader or compliance owner to ensure these practices are regularly followed.

2. Strengthen Access Controls and Empower Employees

Implementing strong access controls is one of the most effective ways to protect patient information. Practices should use role-based access controls, require multi-factor authentication, and enforce strong password policies to ensure users can only access the data necessary for their roles. Given that human error remains a leading cause of security incidents, ongoing cybersecurity training and clear reporting procedures should be key components of every organization's security strategy.

3. Secure EHRs, Practice Management Systems, and Connected Devices

As medical practices continue to adopt interconnected technologies, every device becomes a potential entry point for cyber threats. Regular software updates, encryption, automatic logouts, and mobile device security measures can help protect sensitive data and reduce risk. Healthcare technology should not only improve operational efficiency but also help safeguard patient information across clinical and administrative workflows.

4. Protect Infrastructure and Ensure Business Continuity

As cyber threats continue to evolve, healthcare organizations are investing more in security preparedness. In fact, 72% of medical group practices increased cybersecurity spending in 2024 to better protect against threats and keep critical operations running smoothly if a cyberattack occurs. Regularly securing networks with firewalls, intrusion detection tools, encrypted backups, and tested disaster recovery plans can help practices minimize risks and maintain operations during disruptions.

5. Prepare for Cyber Incidents and Manage Third-Party Risk

A strong cybersecurity strategy includes preparing for incidents before they happen and carefully managing third-party risk. Practices should regularly test response plans, understand HIPAA breach requirements, and evaluate vendor risks such as unauthorized data access, weak security controls, or third-party breaches that could expose patient information. Working with healthcare technology partners that prioritize security and compliance can help reduce risk and strengthen organizational resilience.



Ready to revolutionize your practice's security?

Learn how Greenway Secure Cloud powered by AWS can help protect patient data, support compliance initiatives, and keep your practice running smoothly.

[Learn More](#)