Rectangle HEALTH

Healthcare payment data security.

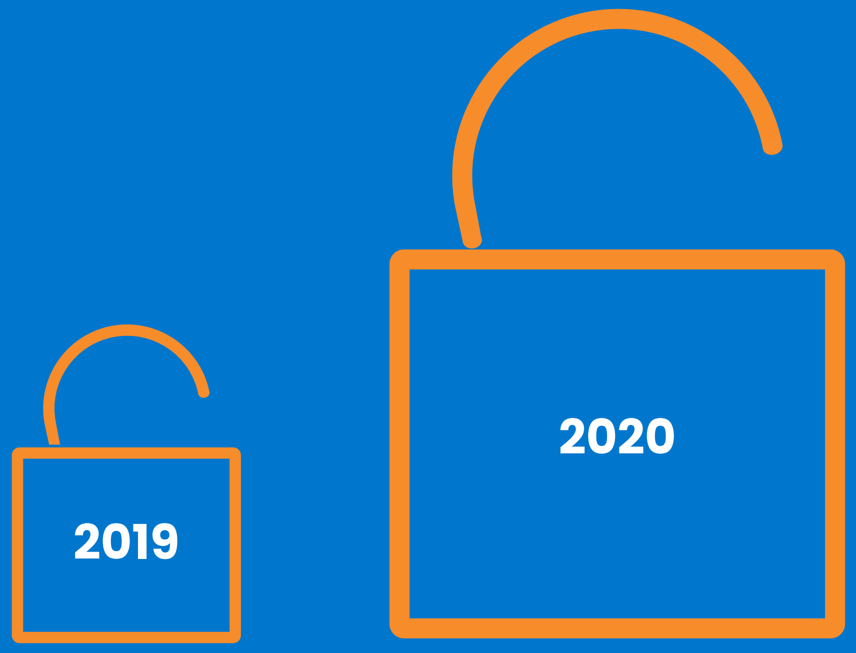
Proactively protecting your practice and your patients.

Introduction

If you were to perform triage on the competing priorities of managing a healthcare office, the security of your patients' personal, health, and financial data would sit at a very urgent level.

Healthcare is consistently at the top of the list of industries affected by data breaches because patient information, with its wide array of data points, is highly valuable and can be vulnerable to misuse. This is the eleventh consecutive year healthcare had the highest cost of a breach.[1] Data thieves are becoming more creative and advanced, and the numbers of healthcare organizations attacked–plus the fees associated–continue to rise.[2] These high costs are often associated with new software implementation, legal fees, PR and communication, reputation repair, and governmental fines.

The security of patient data, including payment information, is critical to your patients' privacy, your organization's reputation among patients and peers, and to your financial well-being. This e-book covers the state of healthcare payment data threats and measures you can take to better protect your practice.



In 2020, **cyberattacks** on healthcare more than **doubled.**[2]

$9.23 million

the average **cost of a data breach** in the healthcare industry in 2021, a **29.5% increase** from 2020.[1]

What do healthcare providers need to be aware of?

Healthcare organizations interact with a massive amount of data, ranging from Protected Health Information (PHI) to sensitive financial information, that is susceptible to exposure from human error, internal leaks, and hackers. While the healthcare industry is becoming more and more reliant on technology and connected devices, many provider offices also still depend on simple email and physical mail to distribute billing statements, test results, and more.

Due to the combination of these factors, plus the large number of employees and contractors who have access to systems, healthcare is consistently ranked among the top verticals for data breaches and hacking instances.

In 2020, COVID-19 stretched healthcare offices thin and forced new policies and remote operations into place. In some offices, security was overshadowed by the daily demands of keeping doors open, and data hackers capitalized on the upheaval with large numbers of attacks.

Who is affected?

The biggest breaches are typically the ones that make the news—large organizations with millions of patient PHI and financial information records compromised—but data breaches in healthcare are not limited to a certain practice size. While large organizations have more records to compromise, they also tend to have advanced technology, tighter security measures, and bigger cybersecurity teams, making them a tougher target.

Small- to medium-sized healthcare organizations also store large amounts of sensitive data, yet their networks tend not to be as well protected, which makes cyberattacks much easier to achieve and still highly profitable for the thief.

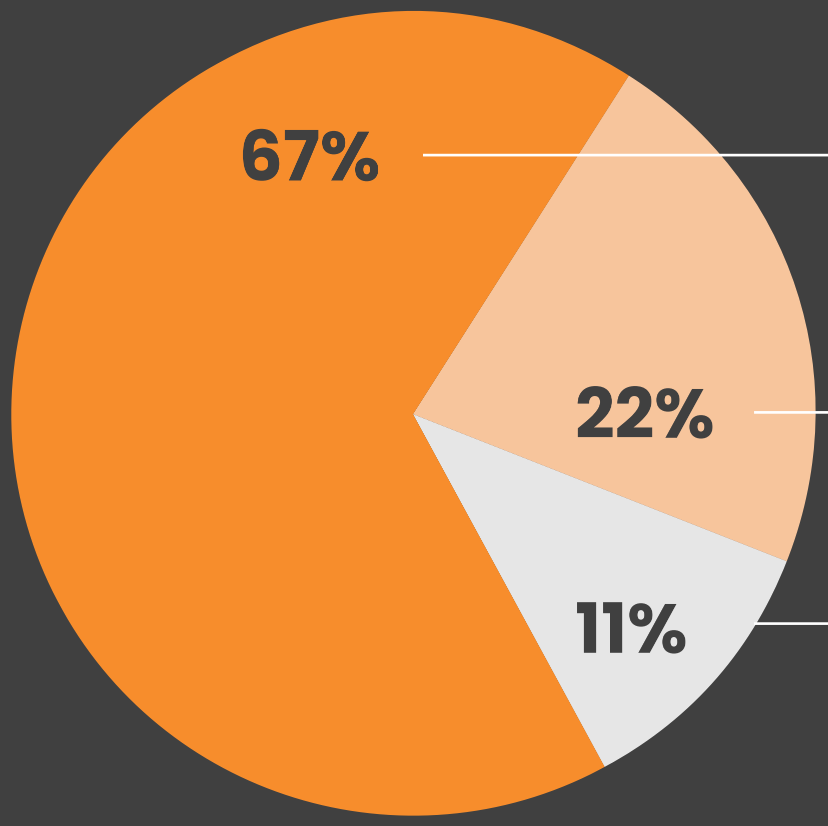
More than 70% of ransomware attacks on healthcare organizations were conducted on practices with fewer than 1,000 employees.[4]

Q3 2020

65.9% of healthcare ransomware attacks were on small- and medium-sized practices.[4]

Q4 2020

In 2020:



Hacking/IT-related data breaches accounted for 67% of all reported healthcare breaches.

Unauthorized access and disclosure incidents accounted for 22% of the breaches.

Theft, improper disposal, and loss followed.[5]

What is the biggest threat?

In 2021, human error occupied the top spot for the most common data breach threat in the healthcare industry. "The most common error continues to be misdelivery (36%), whether electronic or of paper documents."[6] The two main categories of misdelivery are emails that are sent to the wrong address and mass mailings with envelopes addressed to recipients who do not match the contents of the mail.[7] While this type of error can have serious repercussions, it is also possible to reduce or avoid these circumstances by taking preventative measures that include verifying recipient information before sending.

73%

of health system, hospital, and physician organizations report that their **infrastructures are unprepared** to respond to a data breach.[8]

What can you do?

Protect data and prioritize education.

1. According to the PCI Security Standards Council, the best protection against data breaches is not to store card data at all. This includes protecting:
   - Card readers
   - Point-of-sale systems
   - Networks and wireless access routers
   - Payment card data storage and transmission
   - Payment card data stored in paper-based records
   - Online payment applications and shopping carts
2. Commit to meeting and maintaining HIPAA and PCI compliance.
3. Utilize secured digital technology instead of paper for billing statements and patient communications.
4. Provide ongoing education to employees on common risks. For example, train staff to recognize phishing emails and suspicious links and attachments.
5. Use encrypted technology that maintains all necessary compliance requirements and that protects data whether your employees are on premises or remote.
6. Partner with a technology provider to help protect data and provide education.

What to look for in a technology partner.

With the clear threat of cyberattacks and other data breaches, and the potentially catastrophic consequences of being affected by one, it's imperative to choose healthcare technology partners that understand the risks, that continuously take measures to protect your organization's data, and that make it easier for you to meet compliance requirements.

- ✓ Cloud-based Computing
- ✓ HIPAA Compliance
- ✓ PCI Compliance
- ✓ Point-to-Point Encryption (P2PE)

Cloud-based Computing

A significant number of healthcare organizations are planning to either keep certain employees remote, or to keep processes in place that will allow an easier transition to remote work in the future.

There is a shift from on-premises operations for functions such as revenue cycle management, scheduling, and even healthcare visits through telehealth. Moving to a work-from-anywhere model can open the door to new security vulnerabilities.[9]

Cloud-based technology is enabling the new flexible workforce paradigm. Cloud computing not only allows users to access information remotely, but it also includes backup automation and disaster recovery options. In the case of a breach, healthcare providers can use cloud computing so they won't lose any data and can minimize downtime for their staff.

Most current cloud providers offer security, risk management, and monitoring services to protect their users from unauthorized access and breaches.[9]

33%

of CFOs and revenue cycle leaders are **planning for more permanent work-from-home** options based on how COVID-19 impacted their organizations.[11]

HIPAA Compliance

As a part of the healthcare sector, you are already familiar with HIPAA and the importance of staying compliant. Can your technology providers say the same? If your office and patient technology does not specify that it is HIPAA-compliant, sensitive patient health information could be at risk of being exposed. According to the standards set forth by the U.S. Department of Health and Human Services, PHI covers all “individually identifiable health information,”[12] which specifically includes demographic information such as name and address, as well as credit card numbers. Any piece of information that can be traced back to an individual is subject to HIPAA regulations.

Additional considerations for payment technology

PCI Compliance

The Payment Card Industry (PCI) Data Security Standards (DSS) is a set of policies and procedures that businesses must adhere to when these organizations accept credit or debit cards for payment. It is the ongoing responsibility of healthcare organizations to confirm their PCI compliance with yearly assessments. A payment processing partner that understands PCI requirements and guarantees their own compliance makes it easier for your organization to become and stay compliant and can even complete compliance requirements on your behalf.

Point-to-Point Encryption (P2PE)

To meet P2PE requirements, payment card data must be encrypted immediately at the point-of-sale terminal, and it cannot be decrypted until after it is securely transported to and processed by the payment processor. PCI-validated P2PE solutions minimize the burden that practices must bear on an annual basis to obtain PCI compliance by "reducing PCI scope," which means decreasing the amount of cardholder information that a practice possesses.

P2PE solutions help to cut down the "scope" or range of data that can be compromised. This level of encryption prevents clear-text cardholder data from being available in the point-of-sale device or in the practice's system, where it could be exposed to malware.

> **We are committed to providing the most secure and compliant healthcare technology to our family of healthcare clients. P2PE validation is evidence of that commitment."**
>
> – Michael Peluso,
> Chief Technology Officer,
> Rectangle Health

Rectangle HEALTH

Partner with Rectangle Health for industry-leading healthcare payment and administrative technology.

We are committed to routine compliance assessments and work with a leading outside security advisor that is certified by the PCI Security Standards Council.

Cloud-based

Cloud computing is generally considered more cost-effective and secure than traditional methods of electronic records retention and processing because many of the established cloud providers—Microsoft, Google, and Amazon—devote considerable resources toward security.

HIPAA Compliant

We specialize in HIPAA-compliant payment software and payment data security for healthcare organizations. We keep PHI safe by storing all customer data in a secure, encrypted vault that is protected by layers of industry-leading technology. Sensitive information is not held on your premises or stored on your servers or computers.

PCI Compliant

We stay on top of policy and work diligently to support your organization through the often arduous and time-consuming compliance process. With Rectangle Health, your POS systems will be safe from tampering; antivirus software and firewalls will be properly configured and installed; and system weaknesses will be detected.

P2PE Solution

We are recognized by the Payment Card Industry (PCI) Security Standards Council (SSC) as an official Point-to-Point Encryption (P2PE) Solution Provider. PCI validation of P2PE minimizes the processes that practices must go through on an annual basis to obtain PCI compliance.

Rectangle HEALTH

Partner with Rectangle Health for industry-leading healthcare payment and administrative technology.

> ***Rectangle Health is one of only roughly a dozen healthcare payment solution providers that protect data with true point-to-point encryption.***[14]

Additional security features:

Our online payment portal for patients uses reCAPTCHA to reduce fraud and encrypts information that goes through the site, such as credit card details and sensitive data that patients share during the checkout process. We offer regular fraud monitoring to detect irregularities. Patient card information is tokenized and stored in a secure Vault for card-on-file functionality without readable card information ever being stored in the system.

HIPAA COMPLIANT

PCI DSS COMPLIANT

P2PE PCI VALIDATED

EMV & NFC CAPABLE

Conclusion

As healthcare cyberattacks and breaches continue to pose a significant threat, medical and dental offices' awareness and security efforts need to remain vigilant. As healthcare offices are striving to regain what was lost in 2020 and potentially settle into longer term work-from-home and flexible location policies, now is the time to build proactive policies and procedures for data security to protect your reputation and your patients.

Investing in cloud-based technology that offers advanced security and compliance assurance will pay off. Combined with cybersecurity and best-practice training efforts for staff, secure technology can guard you from costly breaches.

Partner with technology providers that have robust security accreditations and that make it easier for your practice to verify compliance. Including proven partners like Rectangle Health in your practice will give your staff–and your patients–confidence and peace of mind that PHI and payment data is protected.

About Rectangle Health

Rectangle Health, a leading healthcare technology company, empowers medical, dental, and specialty practices with seamless and secure technology to drive revenue by increasing patient payments and streamlining practice management and payment processing. Since 1993, the company's innovative solutions have reduced administrative burden and rebalanced the ledger for its thousands of healthcare providers in the United States, reliably processing billions of dollars in payments annually.

To learn more, visit: **www.rectanglehealth.com**.

Notes

1. IBM. (2021). Cost of a Data Breach Report 2021. Retrieved from https://www.ibm.com/security/data-breach

2. Davis, J. (2021, February 25). Healthcare cyberattacks doubled in 2020, with 28% tied to ransomware. Health IT Security. Retrieved from https://healthitsecurity.com/news/healthcare-cyberattacks-doubled-in-2020-with-28-tied-to-ransomware

3. Ellis, D. (2016). How Much Does a Data Breach Cost Your Organization? Security Metrics. Retrieved from https://www.securitymetrics.com/blog/how-much-does-data-breach-cost-your-organization

4. HIPAA Journal. (2021, March 5). Small and medium sized practices under increased pressure from cyberattacks. Retrieved from https://www.hipaajournal.com/small-and-medium-sized-practices-under-increased-pressure-from-cyberattacks/

5. HIPAA Journal. (2021, March 3). 2020 Healthcare Data Breach Report. Retrieved from https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/

6.Bassett, G., Hylender, C. D., Langlois, P., Pinto, A., & Widup, S. (2021). Verizon Business 2021 Data Breach Investigations Report. Retrieved from https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

7. Bassett, G., Hylender, C. D., Langlois, P., Pinto, A., & Widup, S. (2020). Verizon Business 2020 Data Breach Investigations Report. Retrieved from https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report

8. Black Book Research (2020, November 13). Attacks predicted to triple in 2021, Black Book state of the healthcare PR industry cybersecurity industry report. PR Newswire. Retrieved from https://www.prnewswire.com/news-releases/attacks-predicted-to-triple-in-2021-black-book-state-of-the-healthcare-industry-cybersecurity-industry-report-301172525.html

9. Bonderud, D. (2021, March 8). 4 healthcare technology trends expected to boom during COVID-19. Technology Solutions That Drive Healthcare. Retrieved from https://healthtechmagazine.net/article/2021/03/4-healthcare-technology-trends-expected-boom-during-covid-19-perfcon

10. Douglas, M. (2020, August 28). Top 6 benefits of cloud computing for healthcare. Outsystems. Retrieved from https://www.outsystems.com/blog/posts/cloud-computing-in-healthcare/#:%7E:text=Cloud%20computing%20not%20only%20allows,the%20downtime%20for%20their%20staff

11. LaPointe, J. (2020, September 15). Health systems considering remote revenue cycle management. RevCycle Intelligence. Retrieved from https://revcycleintelligence.com/news/health-systems-considering-remote-revenue-cycle-management

12. U.S. Department of Health & Human Services. (2003). Summary of the HIPAA Privacy Rule. HHS.gov. Retrieved from https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

13. Verizon. (2021). 2020 Payment Security Report. Retrieved from https://enterprise.verizon.com/resources/reports/2020-payment-security-report.pdf

14. PCI Security Standards Council. (2021). PCI Point-to-Point Encryption (P2PE)™ solutions. PCI Security Standards Council®. Retrieved from https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

Rectangle HEALTH

Innovation That Drives Patient Payments