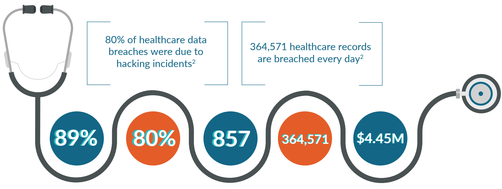
patient FOCUS

Redefining Security Standards: Elevating Compliance in Patient Pay

Your billing office knows how to handle common threats to practice operations: rising claim rejections, changing CPT codes, and other financial hurdles. But there's a new threat on the horizon — and it can dig a much deeper hole in your bottom line than any billing inefficiency.

The Era of Healthcare Cyber Attacks Is Here

Running a successful practice is no longer just about maximizing payments and minimizing delays. Now, the very data you use to manage your practice is at stake, and losing it can cause permanent damage to your practice's profitability and



89% of healthcare organizations have experienced a data breach[1]

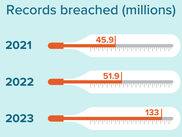
80% of healthcare data breaches were due to hacking incidents[2]

857 data breaches are still under investigation[2]

364,571 healthcare records are breached every day[2]

$4.45 million average cost of a healthcare data breach[3]

The number of breached healthcare records nearly tripled from 2021 to 2023[2]



The Multi-Million Dollar Consequences

The costs of a data breach extend far beyond the resources required to recover patient information and shore up your security protocol. HIPAA violation penalties can reach over $2 million each year.[2]

One of the largest health insurance companies paid a **$16 million** settlement for a breach that exposed **78.8 million** patient records[2]

What It Takes to Keep Payments & Information Secure

Cybersecurity is no longer a simple box to check for your practice. Fortifying your practice and building cyber resilience demands a surround-sound approach, going above and beyond basic standards for compliance.

At PatientFocus, our patient-pay solution leverages a holistic compliance strategy to safeguard your critical healthcare billing data from start to finish, with six core components:

PCI DSS Compliance
Payment Card Industry Data Security Standards (PCI DSS) hold practices accountable for safe and secure credit card processing, protecting sensitive data from data breaches, fraud, and identity theft.

DTMF Masking
When patients enter credit card data on their phone keypad, dual tone multi frequency (DTMF) masking replaces entry tones with monotones to prevent decryption and hacking from unauthorized users.

HIPAA Compliance
The Health Insurance Portability and Accountability Act (HIPAA) heavily regulates and ensures the privacy and security of protected health information.

CFPB Compliance
Compliance with the Consumer Financial Protection Bureau (CFPB) requires accurate, timely, and upfront communication efforts to collect medical payments.

TCPA Compliance
Maintaining compliance with the Telephone Consumer Protection Act (TCPA) requires obtaining consent to contact patients regarding their healthcare or medical information.

CEH Certified Team Lead
The Certified Ethical Hacker (CEH) acts on behalf of the practice as a "hacker" who helps identify and address weaknesses and vulnerabilities in their cybersecurity system.

Maximize Cybersecurity and Revenue Growth With One Billing Solution

Partner with a security-first patient-pay company to get the best of both worlds: state-of-the-art cybersecurity and a measurable increase in revenue growth. Through a unique combination of patient billing expertise and robust cybersecurity protocols, PatientFocus can help your practice build a cyber-resilient practice while achieving:

95% decrease in inbound patient pay calls

40% average increase in patient pay revenue

28% average decrease in days in A/R

Can Your Practice Afford a Patient-Pay Data Breach?

In most cases, the answer is "no" — but the good news is that you never have to find out. With PatientFocus, you gain total peace of mind that your patient billing process upholds the same dedication to cybersecurity as the rest of your practice, providing comprehensive protection for your data, your patients, your practice, and your bottom line.

Increase Revenue With a Secure Patient-Pay Solution

patient FOCUS

www.patientfocus.com | (855) 661-4384

References:

1. *Alder, S. (2016, May 13). Ponemon: 89 Percent of Healthcare Organizations Have Experienced a Data Breach. The HIPAA Journal. https://www.hipaajournal.com/ponemon-89-pc-healthcare-organizations-experienced-data-breach-3430/*
2. *Alder, S. (2024, July 18). Healthcare Data Breach Statistics. The HIPAA Journal. https://www.hipaajournal.com/healthcare-data-breach-statistics/*
3. *Alder, S. (2023, July 24). IBM: Average Cost of a Healthcare Data Breach Increases to Almost $11 Million. The HIPAA Journal. https://www.hipaajournal.com/2023-cost-healthcare-data-breach/*