Looking to avoid risk?

WE CAN SHOW YOU THE WAY.

TOP BUSINESS RISKS FOR MEDICAL PRACTICES

THE DOCTORS COMPANY

medical ~~mal~~practice insurance

YOUR PRACTICE IS AT RISK

As a healthcare employer you are at risk for more than just a malpractice suit—other exposures are associated with billing, cyberattacks, employment-related claims, and audits. It's important to know these threats to your practice, as well as preventative steps you can take.

YOUR RISKS AS A HEALTHCARE EMPLOYER

Do you know what the most severe exposure is to your practice outside of malpractice suits? Employment-related claims.

Your role as an employer poses an ever-increasing risk. In a 5 year period, 6 out of 10 employers can expect a claim based on harassment, discrimination, retaliation, wrongful termination, wage and overtime practices, or a host of other actions you take as an employer.[1]

And remember, as an employer, you're not only liable for your actions—you're also responsible for the actions of your employees.

If a charge is filed against you, even one that is frivolous, you would have to pay to defend yourself and your practice. Doctors are a particular target for employment-related lawsuits because they are viewed as having deep pockets.

THE SCOPE OF EMPLOYMENT-BASED CLAIMS

What is the scope of employment-based claims? Here are some alarming statistics:

- The number of charges filed with the Equal Employment Opportunity Commission (EEOC) for the most common claim, retaliation, rose by 67 percent over the last 10 years.[2]
- The median award in employment practices lawsuits was $325,000 in 2012.[3]
- The probability of a plaintiff winning an employment practices claim at trial is 51 percent.[4]

In a 5 year period, 6 out of 10 employers can expect a claim based on harassment, discrimination, retaliation, wrongful termination, wage and overtime practices, or a host of other actions you take as an employer.

4 STEPS TO REDUCE THE LIKELIHOOD OF EMPLOYMENT-RELATED LAWSUITS

Given this environment, what can you do to mitigate your exposure to employment-related lawsuits? Here are four steps every medical practice should take:

1. Create, document, and use enforceable employment procedures.
2. Have your employment procedures reviewed at least every two years by a lawyer or human resources professional.
3. Train your managers and supervisors on your procedures.
4. Adopt an equitable format and policy for administering evaluations.

Along with following these steps, you can protect yourself and your practice from claims brought against you by employees or prospective employees by purchasing employment practices liability insurance (EPLI).

EPLI protects you from employment-related claims, including wrongful acts such as harassment, discrimination, retaliation, or workplace torts. Workplace torts, which fall outside of workers' compensation coverage, can include employment-related misrepresentation, negligent evaluation, wrongful discipline, and wrongful deprivation of a career opportunity.

You can extend your EPLI coverage to ensure you are protected against third party discrimination or harassment claims from a customer or vendor.

Case Study: Prospective Employee Denied Employment

This case involves a physician who was not even an employee. In this incident, a medical group offered employment to a physician who then sought privileges at a local hospital. The hospital refused to grant privileges to the physician based on a medical condition. As a result, the medical group rescinded its offer of employment.

The physician filed a charge of discrimination with the EEOC against both the medical group and the hospital under the Americans with Disabilities Act. The physician alleged he was denied an employment opportunity on the basis of disability.

Even though the hospital did not employ the physician, the EEOC found sufficient evidence to establish a violation of the Americans with Disabilities Act by the hospital in denying the physician's application for privileges. The case settled for $65,000 and the total defense costs were approximately $95,000.

MEDICAL BILLING AND CODING RISKS—YOU COULD FACE AN AUDIT

All healthcare providers who submit bills for reimbursement to the government or private insurance payers are susceptible to an audit, which could lead to fines and penalties.

The CMS Recovery Audit Program, which reviews and corrects hospital billing errors, has successfully recovered more than $7 billion in improper Medicare payments since it began in 2009.[5] As a healthcare provider, you could incur considerable expense if potential errors are found. On average, physicians and healthcare organizations spend $80,000 in defense of alleged billing errors. In addition, fines and penalties could reach hundreds of thousands of dollars.[6]

The two biggest exposures discovered through government billing audits are improper coding and exaggerated coding. Improper coding refers to discrepancies between the code submitted and the rest of the information provided for a claim, while exaggerated coding indicates billing for a level of service that is higher than the service performed.

Government audits focus on services that appear to have been billed twice—similar services or the exact service—on the same claim form.

Coding and billing discrepancies can also lead to problems with private insurance payers. Submitting claims that are not properly coded can tarnish a physician's reputation with third party payers, likely leading to more denied claims or improperly down-coded claims.

On average, physicians and healthcare organizations spend $80,000 per proceeding in defense of alleged billing errors. In addition, fines and penalties could reach hundreds of thousands of dollars.

7 STEPS TO MITIGATE BILLING ERRORS AND OMISSIONS

What can you do to mitigate your risk of billing errors and omissions? Here are seven steps every medical practice should take:

1. Establish compliance standards, and conduct internal monitoring and auditing of those standards.
2. Stay current on coding rules and federal regulations by reading the Federal Register at federalregister.gov/ and Health and Human Services bulletins at oig.hhs.gov/compliance/alerts/bulletins/.
3. Identify billing issues, track denied claims, look for patterns, and take necessary actions to avoid improper payments.
4. Conduct appropriate training for your staff.
5. Use updated coding standards, including Current Procedural Terminology, a Healthcare Common Procedure Coding System, and new ICD-10 codes.
6. Consider using a medical coding and billing software program.
7. Have an expert conduct a thorough analysis of your practice to ensure no exposure goes uncovered.

ADDITIONAL CONSIDERATIONS

In addition to following these seven tips, review your medical liability policy to ensure it includes adequate protection against legal and audit expenses, as well as fines and penalties associated with billing errors, HIPAA, EMTALA, or Stark proceedings.

Ask yourself these questions to mitigate your risk for errors and ensure you are prepared in the event of an audit:

- Do your billing, coding, and privacy procedures meet current standards?
- Is your staff properly trained?
- Are you and your staff protected against a whistleblower complaint from a patient or employee?
- Does your coverage include a shadow auditor?

Case Study: Incorrect Website Coding

A plastic surgeon posted before and after photos of her patients on her website. However, the code for the website was written incorrectly and the photos that were posted accidentally exposed the patients' personal information. Legal settlements per patient have exceeded $150,000. Fifteen claims have been filed and fifteen additional claims are expected, with a total cost of over $4.5 million.

HEALTHCARE DATA BREACH RISKS

Cybercrime costs the U.S. economy billions of dollars each year. But one business segment is attacked more than any other: healthcare. A full 51 percent of breaches occur in healthcare entities.[7] The healthcare industry is targeted for two main reasons:

- Healthcare organizations fail to upgrade their cybersecurity as quickly as other businesses.
- Criminals find personal patient information particularly valuable to exploit. Cybercriminals are paid $20 each for health insurance credentials, compared to only $1 to $2 each for credit card numbers.[8]

YOU ARE AT RISK FOR A DATA BREACH

In the last 2 years, 94 percent of healthcare organizations have had at least 1 data breach. And the average cost of dealing with those breaches was $2.4 million.[9]

Your patients' HIPAA-protected healthcare data is at risk. It could be stolen, lost, or accidentally transmitted. Your network is also vulnerable to high-tech black market attacks.

In the last 2 years, 94 percent of healthcare organizations have had at least 1 data breach. And the average cost of dealing with those breaches was $2.4 million.

8 STEPS TO MITIGATE YOUR RISK AND EXPOSURE TO CYBERATTACKS AND DATA BREACHES

Will you have a data breach or hack? Yes. It is not a question of if, but when. What can you do to mitigate your risk and exposure to cyberattacks and data breaches?

1. Develop a data recovery and/or disaster plan.
2. Create, document, and use enforceable cyber and data breach procedures.
3. Train your staff on your procedures.
4. Encrypt all computers and devices with passwords that are composed of numbers, letters, and symbols.
5. Protect your facilities by securing building access, shredding documents, and installing firewalls.
6. Have separate office and guest Wi-Fi networks in your office and/or practice.
7. Install endpoint security software, including antivirus, antispyware, and antimalware.
8. Buy insurance coverage to mitigate your risk.

Case Study: Software with Security Defects

A provider contracted with a software vendor to develop and maintain an online appointment scheduling system that would capture demographics and other personal patient health information. The vendor did not properly secure the website. As a result, the patient information was viewable by unauthorized users visiting the site.

A complaint was filed by a patient against the provider, who was instructed to shut down the website. The provider contacted the software vendor, who promptly corrected the defects in the program. However, the provider had to pay $42,000 in defense costs.

PROTECTING PRACTICES AGAINST EMERGING RISKS IS JUST ONE WAY WE'RE TAKING THE MAL OUT OF MALPRACTICE INSURANCE

Founded and led by physicians, The Doctors Company is relentlessly committed to advancing, protecting, and rewarding the practice of good medicine. The Doctors Company partners with practices of all sizes to help them manage the complexities of today's healthcare environment by providing expert guidance, resources, and coverage. The Doctors Company is the nation's largest physician-owned medical malpractice insurer, with 79,000 members and over $4 billion in assets, and is rated A by A.M. Best Company and Fitch Ratings.

Our medical malpractice insurance includes protection against HIPAA privacy breach allegations through CyberGuard® cyber liability coverage, and against Medicare reviews through MediGuard® regulatory risk coverage. And our EPLI offers protection against employment-related claims—including wrongful termination, discrimination, whistleblower, and breach of an employee's federal, local, and state rights.

Don't put your practice at risk. Protect your business—learn more at **thedoctors.com**.

---

[1]Employment practices liability insurance. The Hartford. http://www.thehartford.com/commerical-insurance-agents/small-businessemployment-practices-liability-insurance. Accessed August 3, 2015.

[2]Retaliation-based charges: FY 1997-FY 2014. U.S. Equal Employment Opportunity Commission. http://www.eeoc.gov/eeoc/statistics/enforcement/retaliation.cfm. Accessed August 3, 2015.

[3]Employment practice liability trends hit new high. HR that Works. January 17, 2013. http://www.hrthatworksblog.com/2013/01/17/employment-practice-liability-jury-award-trends-hit-new-high/. Accessed August 3, 2015.

[4]Complete the picture: A spotlight on the United States Employment Practices Liability Insurance market. Advisen Insurance Intelligence. September 2014. http://www.aig.com/Chartis/internet/US/en/Advisen_whitepaper_final_tcm3171-642387.pdf. Accessed August 3, 2015.

[5]CMS reports high accuracy of RAC audits. Reuters. December 5, 2013. http://www.reuters.com/article/2013/12/05/achci-on-cms-report-idUSnBw056171a+100+BSW20131205. Accessed August 3, 2015.

[6]Smigel T. The facts about billing errors & omissions insurance. *Oregon HealthCare News*. http://www.orhcnews.com/newsletters/or-tsmigel0911.pdf. Accessed August 3, 2015.

[7]Visser S, Osinoff, G, Hardin B, et al. Information security & data breach report—March 2014 update. Navigant. March 31, 2014. http://www.navigant.com/~/media/WWW/Site/Insights/Disputes%20Investigations/Data%20Breach%20Annual%202013_Final%20Version_March%202014%20issue%202.ashx. Accessed August 3, 2015.

[8]Cybercrime and the healthcare industry. EMC. July 2013. http://www.emc.com/collateral/white-papers/h12105-cybercrime-healthcare-industry-rsa-wp.pdf. Accessed August 3, 2015.

[9]2014 cost of data breach study: United States. Ponemon Institute LLC. May 2014. Study sponsored by IBM. http://www.accudatasystems.com/assets/2014-cost-of-a-data-breach-study.pdf. Accessed August 3, 2015.

THE DOCTORS COMPANY
medical ~~mal~~practice insurance