SPECIAL REPORT

5 STEPS TO SAFEGUARD YOUR DIGITAL PRACTICE

The *digital practice*—the electronic storage, access, sharing, and monitoring of health information—promises increased convenience, improved patient care, and lower costs.[1] But this electronic access to medical records also brings with it the risk of cyberattacks and new avenues for employee error or misuse, which could put sensitive patient data at risk of exposure and your practice at risk of violating state and federal regulatory and privacy laws. In this special report, we offer five steps to help you reduce these risks that could compromise confidential medical records and cause financial harm to your practice.

NORCAL GROUP®

> There are only two types of companies:
> Those that have been hacked, and those that will be."
>
> *(Former FBI Director Robert Mueller)*

DATA BREACHES: A POTENTIALLY COSTLY RISK FOR YOUR PRACTICE

A complete medical record is highly valuable to criminals:[3]

$1,000
ON THE DARK WEB

- **$1** for SSN number
- **$5** for credit card/ CVV combination

HEALTHCARE DATA BREACHES ARE COSTLY:[4]

AVERAGE TOTAL COST
$6.45M
65% more than the US average

AVERAGE COST PER RECORD
$429
177% of the US average of $242

DATA BREACHES AFFECT BOTH LARGE AND SMALL ORGANIZATIONS:[5]

50%
— Healthcare organizations experiencing a data breach with 1,000 or fewer employees

THE TOP THREAT ACTIONS ALL INVOLVE EMPLOYEES OR PARTNERS:[5]

1. **Error:** 33.5% (incidents) / 35.1% (breaches)
2. **Misuse:** 29.5% (incidents) / 30.7% (breaches)
3. **Physical (mostly loss/theft)**: 15.6% (incidents) / 16.4% (breaches)*

** 75% of these were theft of a laptop (44%) or paper documents (31%)*

DATA BREACHES COST MEDICAL PRACTICES BUSINESS:[4]

7%
— Abnormal customer turnover after a healthcare data breach

80% higher than the US average

CASE STUDY:

Theft of Unsecured Data Leads to HIPAA Breach Notification

A medical assistant performing a quality audit **downloaded patient records onto her laptop** for review over the weekend. On her way home from work she stopped off for dinner with friends and the laptop was stolen from her car. The data on the laptop were **not encrypted** and there was **no password protection**. Because the clinic could not demonstrate a low probability that the PHI was compromised, the practice was required to comply with the HIPAA breach notification requirements.

This case study is summarized from an issue of NORCAL Group's policyholder publication, *Claims Rx*.

BUILD A CULTURE OF INFORMATION SECURITY WITH THESE 5 STRATEGIES

START WITH COMPLIANCE, BUT DON'T STOP THERE

Compliance can improve your data security posture, but these five strategies can help you build a robust culture of information security in your practice.

1. CONDUCT AN INFORMATION SECURITY "ANNUAL EXAM"

In a dynamic practice environment, a security risk analysis is essential for maintaining a culture of security and is a requirement of the HIPAA Security Rule.[6] Based on your circumstances, you may decide to perform this analysis annually to maintain compliance with state and federal privacy laws and address identified risks. Document the results of the risk assessment for compliance auditing.

2. LOCK DOWN YOUR SYSTEMS AND DATA

Advanced security measures can help protect your systems and sensitive data. Consider enabling login verification (with security cards or fingerprint scans), timed user logouts, and user lockout after failed login attempts. Also, encrypting sensitive data in storage (laptops, servers, and in the cloud) and in transit (file transfers, but also emails and text messages) helps protect sensitive data after a breach[4] and may prevent the need for a HIPAA notification.

3. ACTIVELY MONITOR YOUR DATA

A data activity monitoring system identifies suspicious activity and alerts system administrators to potential security threats. This can help you identify threats and possibly avoid a breach. The HHS OCR HIPAA Audit Protocol is a good place to start for determining monitoring protocols.[6]

4. DEVELOP A BREACH RESPONSE PLAN

You likely have response plans in place for medical emergencies or severe weather events. Take this same care and develop a plan for how to respond to a data breach, with staff roles and communication protocols clearly defined. And, just as fire drills teach people how to respond in an emergency, practicing your breach response with relevant staff can help them know what to do when a breach happens.[4]

5. EDUCATE AND EMPOWER STAFF

The majority of data breaches in healthcare are associated with internal actors being careless or behaving badly—the only industry where this is the case. Through user training, communication, and common sense policies, you can help your staff avoid these errors.[2]

- **Educate:** Use examples and regular training to help staff understand what happens in a data breach and how to avoid one.
- **Communicate:** Keep staff informed about HIPAA rules and data security best practices. Maintain open lines of communication between clinical/administrative staff and IT/security staff.
- **Empower:** Encourage and provide ways for staff to report security breaches or concerns (however small) without fear of blame or recrimination (often accompanied by a policy of reporter anonymity).

Numbered references available at *norcal-group.com/library/preventing-hipaa-data-breaches-to-safeguard-your-digital-practice*

This report is presented as a courtesy by NORCAL Mutual Insurance Company. Our Risk Management Specialists are always ready to help policyholders with risk issues and to support practice changes that lower risk and improve patient safety.

ABOUT NORCAL GROUP

The NORCAL Group of companies provide medical professional liability insurance, risk management solutions and provider wellness resources to physicians, healthcare extenders, medical groups, hospitals, community clinics, and allied healthcare facilities throughout the country. NORCAL Group includes NORCAL Mutual Insurance Company and its affiliated insurance companies. Please visit norcal-group.com/companies for more information.

NORCAL GROUP®

844.4NORCAL | norcal-group.com

ng0673