SPECIAL REPORT

PREVENTING EMPLOYEE ERROR FROM CAUSING A HIPAA DATA BREACH

The healthcare industry experiences the most data breaches of any industry and has the highest proportion of insider sources.[1] Healthcare data breaches are also the costliest, with an average cost of $380 per record — 69% greater than the national average.[2] The good news is that, because more than half of all cybersecurity incidents in healthcare involve the inadvertent actions of employees, there is an opportunity for practices to greatly reduce their risk of attack with employee training and awareness that builds a pervasive "culture of security." In this special report, we offer best practices that can help you guard against inadvertent cybersecurity incidents.

NORCAL GROUP

ProAssurance

HIPAA DATA SECURITY: YOUR EMPLOYEES ARE YOUR BIGGEST RISK

"The Healthcare vertical is rife with Error and Misuse. In fact, it is the only industry vertical that has more internal actors behind breaches than external."[1]

71% OF CYBSECURITY INCIDENTS IN HEALTHCARE **INVOLVE EMPLOYEE ACTIONS**[1]

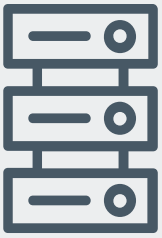
53%
by "inadvertent actors"[1]
(error, physical loss/theft, social/phishing)

18%
by "malicious insiders"[1]
(privilege misuse)

"Healthcare is almost **7** times more likely to feature a causal error [in cybersecurity incidents] than other [industries]."[1]

SENSITIVE PATIENT DATA AT RISK

Data contained in healthcare data breaches:[1]



79% Medical Data
37% Personal Data
4% Payment Data

** Breaches often contain multiple data types so the total does not equal 100.*

62% OF ALL EMPLOYEE ERRORS WERE MISDELIVERY OF PRIVILEGED INFORMATION

misplaced assets, misconfigurations, publishing errors and disposal errors accounted for much of the rest[1]

In instances of intentional misuse, the motives are almost equally divided between reasons of...

FUN OR CURIOSITY (I.E., SNOOPING)
&
FINANCIAL GAIN[1]

$380 =

Average cost of a data breach in the healthcare industry per medical record[2]

69% greater *than the national average*[2]

RANSOMWARE — AN OMINOUS THREAT

CAUSE: Employee opens an attachment or link in spam email

RESULT: Attacker blocks access to critical patient data

DANGER: Patient safety at risk

COST: 10s of thousands of dollars to unlock data

BUILD A CULTURE OF SECURITY TO PROTECT AGAINST EMPLOYEE DATA BREACHES

Because more than half of all cybersecurity incidents in healthcare involve the inadvertent actions of employees, there you have an opportunity to greatly reduce the risk of attack with employee training and awareness. Thinking of information security as not a medical condition with a ready cure but as a chronic illness requiring ongoing treatment, monitoring, testing, and re-evaluation — coupled with these recommendations — can help you build a "culture of security" in your practice.[3]

INSTITUTE ENHANCED STAFF TRAINING & AWARENESS

- ✓ Establish a corporate culture that frowns upon printing out sensitive data.[4]
- ✓ Inform staff that accessing PHI for reasons not related to their job functions is a violation of state and federal privacy law.
- ✓ Provide continual, multifaceted security awareness training that includes training, daily reminders, and visual workplace cues.[3]

ESTABLISH STRONG POLICIES & PROCEDURES

- ✓ Maintain strict security policies with a strong reward/repercussion system:
  - Never share login credentials.
  - Never log in colleagues.
  - Always log out of shared terminals after each use.
  - Turn off (don't simply log out of) computers and shared terminals at the end of the work day whenever possible.
- ✓ Conduct an information security risk analysis "annual exam."[3]
- ✓ Have and enforce a formal procedure for disposing of anything containing sensitive data.[4]
- ✓ Establish a "four-eyes" (two-person review) policy for publishing or sending information.[4]
- ✓ Ensure that all security and data handling policies are task-oriented and easily understood by non-technical staff.
- ✓ Consider "safe harbor" policies that encourage employees to safely report security lapses and suspicious or inappropriate behavior.
- ✓ Enter into a HIPAA business associate agreement as necessary with third-party business partners.

MORE ON THIS TOPIC IS AVAILABLE IN THE NORCAL KNOWLEDGE LIBRARY
at **norcal-group.com/library/** — select Information Security in the topics menu.

Numbered references available at **norcal-group.com/library/preventing-employee-error-from-causing-a-hipaa-data-breach**

This report is presented as a courtesy by NORCAL 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

NORCAL Group, now part of ProAssurance, offers a full spectrum of medical professional liability insurance solutions to physicians and other healthcare providers. NORCAL Group includes NORCAL Insurance Company and its affiliated insurance companies. Please visit norcal-group.com/companies for more information.

844.466.7225 norcal-group.com

ng5093