HIPAA DATA SECURITY:
YOUR EMPLOYEES ARE YOUR BIGGEST RISK

NORCAL GROUP®

"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]
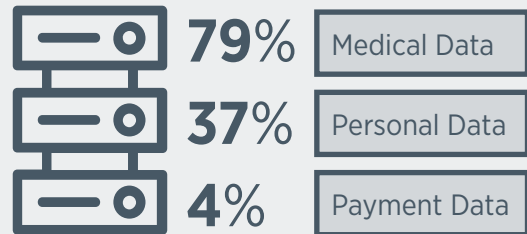*(error, physical loss/theft, social/phishing)*

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]

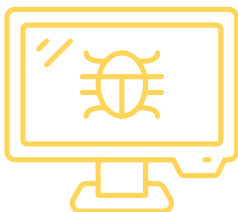In instances of intentional misuse, the motives are almost equally divided between reasons of...

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