

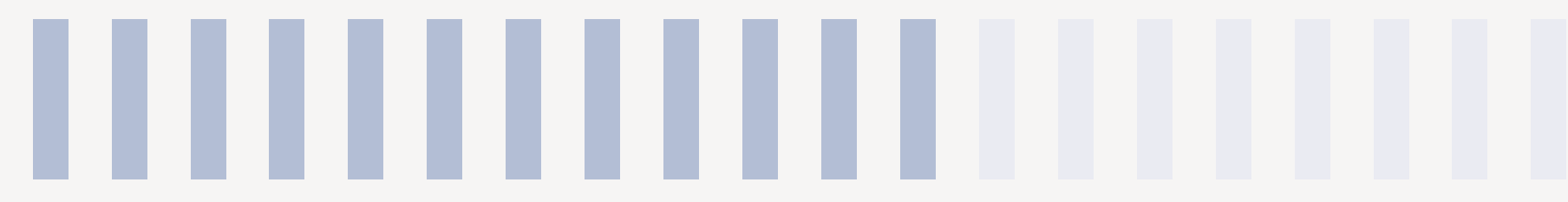
Cracking the Code: Healthcare's Cloud Data Security Hurdles

THREATS, BREACHES, AND RISKS TO DATA IN THE HEALTHCARE INDUSTRY



The healthcare industry consistently ranks among the top five sectors experiencing data breaches, which result in significant financial losses in civil penalties and brand reputation.

Read on to see the numbers behind these breaches and how they can impact your healthcare organisation.



41%

Health information was exposed in 41% of reported breaches, making it the third most commonly affected type of personal information.

MOST COMMON THREATS

- HUMAN ERROR BREACHES
- DATA EXPOSURE
- CYBERSECURITY INCIDENTS
- MALICIOUS ATTACKS
- SECONDARY NOTIFICATIONS



43%

Sending PII to the wrong recipient accounts for 43% of breach-related errors (email and mail errors).



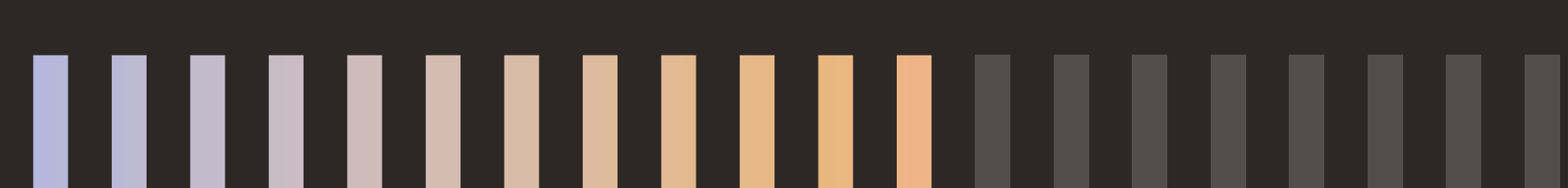
Healthcare Data Privacy Is Crucial

PHI and PII are highly sensitive data sets, making that information a prime target for cyberattacks.



- SENSITIVE NATURE OF DATA
- INCREASING CYBER THREATS
- REGULATORY COMPLIANCE

With steeper regulatory requirements and increasing cloud breach risks, protecting this data isn't just a best practice — it's a necessity for maintaining patient trust and avoiding costly fines.



44%

44% of data breaches resulted from cybersecurity incidents, with phishing being the top cause.

Take a Proactive Approach to Your Healthcare Data Protection

With Protegrity, healthcare organisations can manage and protect patient data with the highest levels of security thanks to:

- COMPREHENSIVE PROTECTION
- CLOUD SECURITY
- HUMAN ERROR MITIGATION
- REGULATORY COMPLIANCE ASSURANCE

STAY **AHEAD** OF BREACHES

WITH PROTEGRITY'S CLOUD DATA PROTECTION SOLUTIONS FOR HEALTHCARE BY VISITING www.protegrity.com