

# 2021 Data Breaches in Healthcare

A CONTINUOUS TREND OF CYBER THREATS IN THE HEALTHCARE INDUSTRY

Healthcare continues to hold **the highest industry cost of a data breach** as the category approached its 11th consecutive year in 2021.

## Average Total Cost

\$9.23 million



2021

\$7.13 million

2020

The average total cost of a data breach in healthcare raised from \$7.13 million (2020) to \$9.23 million (2021). This has resulted in a **29.5% increase**.

## Actor Motives



Intentions of cybercrime activity continue to gear towards financial motivation in the healthcare sector, with the deployment of ransomware being a favored tactic.

91%

FINANCIAL

5%

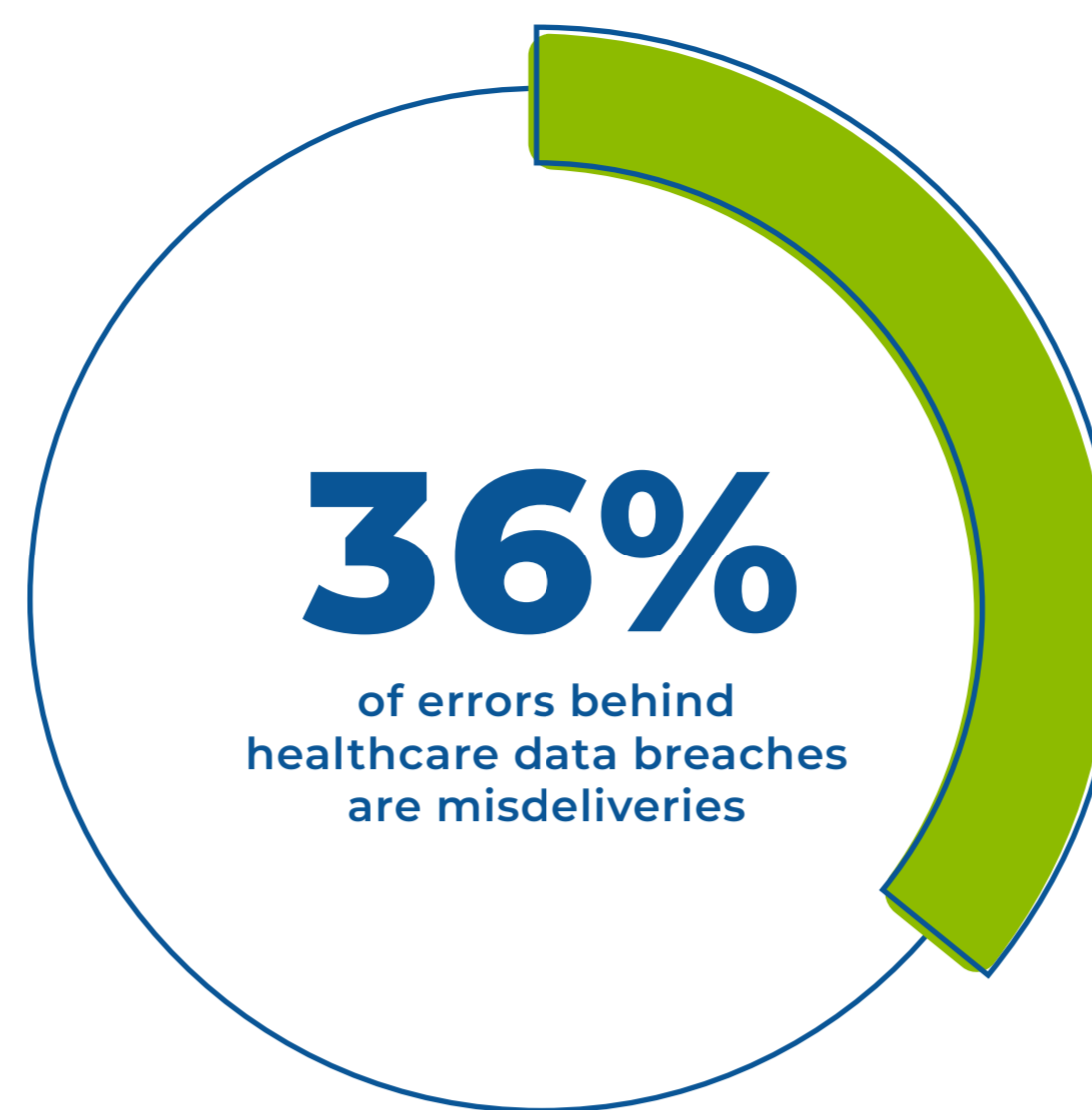
FUN

4%

ESPIONAGE

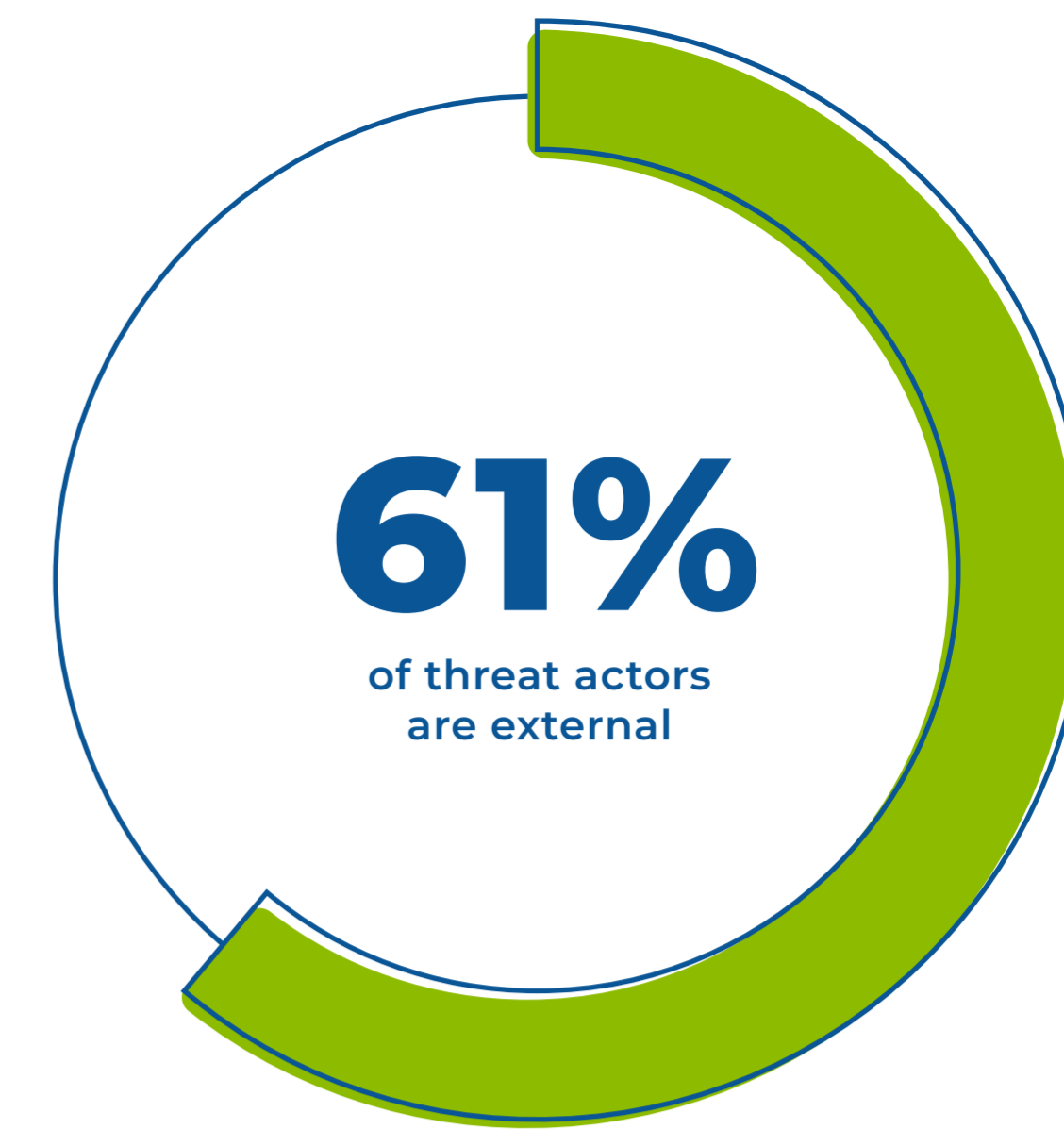
1%

GRUDGE



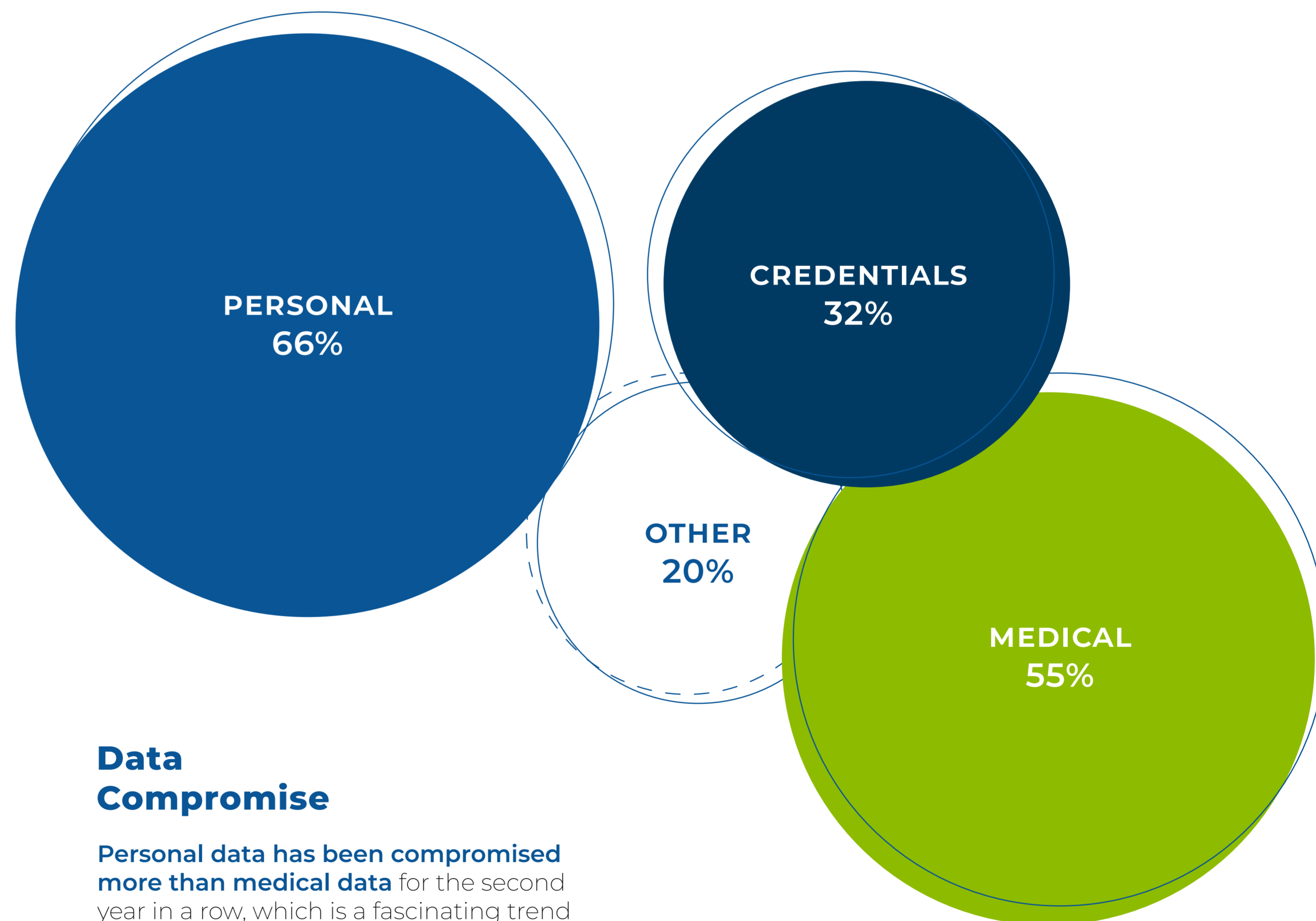
## Errors

Over the past several years, basic human error remains to be a factor that afflicts this sector. Misdelivery continues to be the most common error, making up **36% of the error varieties that occur in breaches**.



## Threat Actors

The healthcare industry has seen a **shift from breaches caused by Internal actors to primarily External actors** since 2019.



## Data Compromise

Personal data has been compromised **more than medical data** for the second year in a row, which is a fascinating trend considering the expectation of seeing more medical information in this sector.

## SOURCE

"Cost of a Data Breach Report 2021 | IBM." IBM - United States, IBM Corporation, 2022, <https://www.ibm.com/security/data-breach>.

"2021 Data Breach Investigations Report." Verizon Business, Verizon, 2022, <https://www.verizon.com/business/resources/reports/dbir/>.