MEDITOLOGY SERVICES

THE RISE OF SOC 2 IN HEALTHCARE

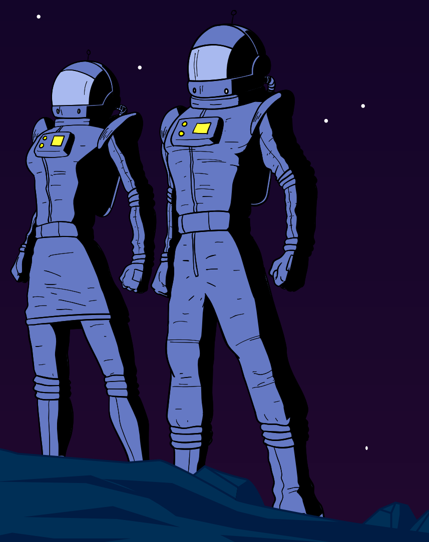
Security breaches from third-party Business Associates and related regulatory penalties are piling up for healthcare entities. The increased dependency and eroding trust with vendors on privacy and security matters has led to a boom in SOC 2 attestations.

WHAT IS DRIVING THE INCREASE IN SOC 2 ATTESTATIONS?

$7.13M per breach

- Healthcare has once again topped the list of the highest average breach cost per industry segment, with an average of $7.13m per breach[1]
- A top source of civil monetary penalties from OCR for Covered Entities involves inadequate management and compliance for third-party Business Associates
- SOC 2 Type 2 reports have become a contractual requirement for third parties looking to do business with many of the nation's leading healthcare organizations
- In the case of an OCR audit, SOC 2 reports help to demonstrate reasonable and appropriate compliance with regulatory requirements that apply to healthcare organizations

WHO IS GETTING SOC 2 ATTESTATIONS?



- Cloud hosting platforms
- Healthcare payers
- Data analytics firms
- Electronic Health Records solutions
- Healthcare SaaS vendors
- Research organizations
- Transcription companies
- Claims processing firms
- Healthcare consulting firms
- Leading healthcare providers
- Many more third-parties servicing the healthcare industry

WHAT SECURITY & PRIVACY CONTROLS ARE INCLUDED FOR SOC 2?

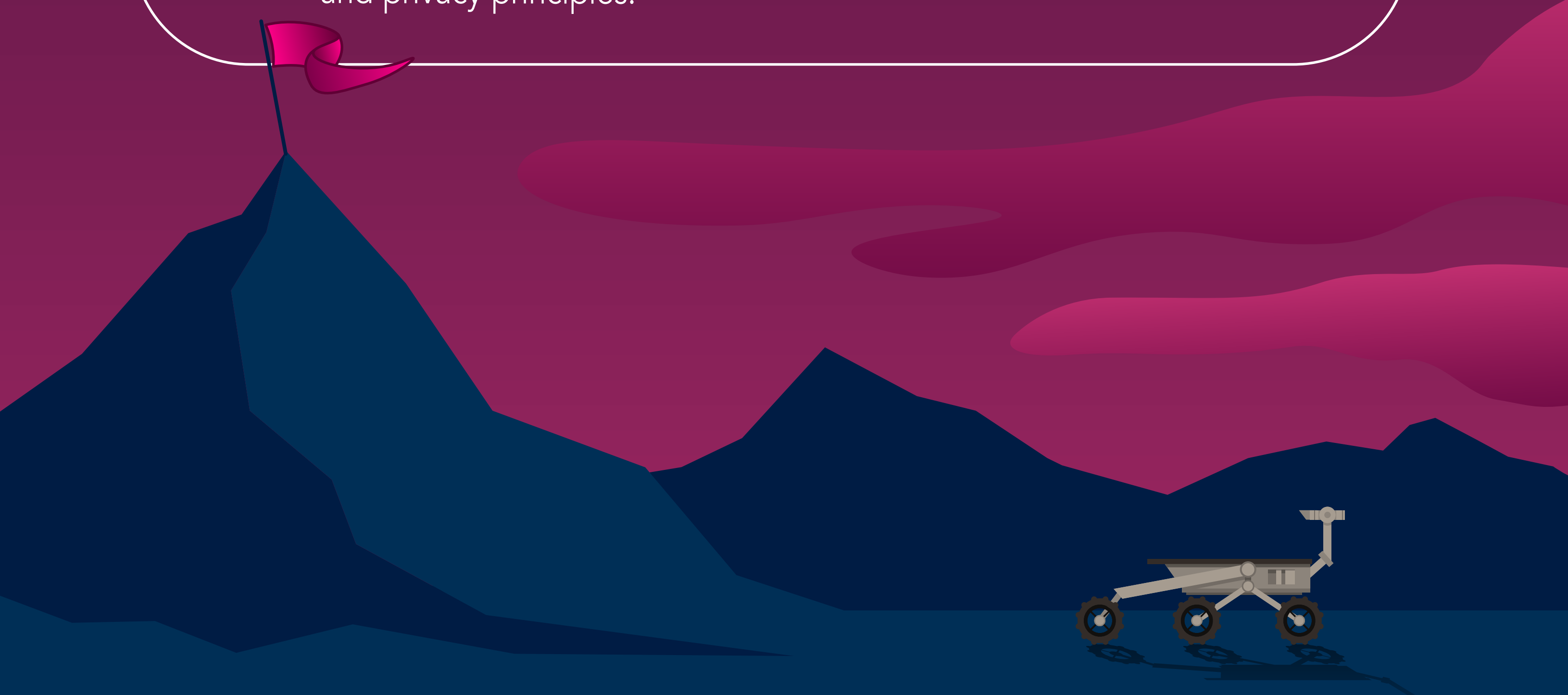
Security refers to the protection of information systems against unauthorized access or disclosure and preventing negative effects on systems which could affect the other trust principles.

Availability controls ensure that information is readily available and that backups and continuity processes are in place to restore services in a timely manner for system outages.

Confidentiality deals with controls which protect the confidentiality of data. This includes agreements and assessments with third parties regarding confidentiality.

Processing Integrity deals with making sure that system processing is complete, accurate, timely, and authorized.

Privacy ensures that information is collected, used, retained, disclosed in conformity with commitments to entity's privacy notice and privacy principles.



WHAT ARE CRITICAL SUCCESS FACTORS FOR A SUCCESSFUL SOC 2 ENGAGEMENT?

○ Have the right stakeholders involved early on in the process
○ Form a governance committee and hold periodic status meetings
○ Conduct a readiness assessment
○ Review the report for accuracy
○ Perform periodic internal reviews
○ Apply recommendations

[1] Healthcare Breach Trends: Analysis of the 2020 IBM & Ponemon Data Breach Report

Meditology Services is a top-ranked provider of information risk management, cybersecurity, privacy, and regulatory compliance consulting services, exclusively for healthcare organizations. Our Meditology Assurance division is an AICPA accredited provider of SOC 2 auditing, reporting, and attestations.

MEDITOLOGY SERVICES
info@meditologyservices.com
MEDITOLOGYSERVICES.COM