INFOGRAPHIC

Time. Money. Trust.

Find out what opportunities — and challenges — lie ahead for security and compliance in healthcare.

The simultaneous rise of cyberattacks and healthcare digital touchpoints, such as those of telehealth and mobile apps, makes this a crucial moment for providers.

57%

increase in cyberattacks against U.S. organizations from 2021 to 2022.[1]

62%

of organizations say their security team is not sufficiently staffed.[2]

207 days

is the average amount of time it takes organizations to identify a data breach.[3]

Along with the **loss of data**, healthcare data breaches also harm team **productivity**, **damage your reputation** and **risk patients' physical safety**.

Adopting new technologies can come with risks.

67%

percent of IT and IT security practitioners in healthcare say technologies such as cloud, mobile, big data and IoT increase the risks to patient information and safety.[4]

Security has a verifiable impact on patient trust.

60%

of patients are concerned about ransomware attacks and data breaches in healthcare.[5]

Data breaches also have a huge financial price.

$10.1M

is the average cost of a healthcare data breach[6]

A dedicated partner can provide you with proactive monitoring, streamlined HIPAA compatibility and 24/7/365 support you can count on. Become more agile in every area of your healthcare organization with security and access you can truly rely on.

Ready to enhance your compliance and security?

Learn more

enterprise.spectrum.com/DigitalHealth

1. "Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks" Check Point Research, January 2023
2. "Cost of a Data Breach Report 2022," IBM and Ponemon Institute, July 2022
3. Ibid
4. "Cyber Insecurity In Healthcare: The Cost And Impact On Patient Safety And Care," Ponemon Institute, March 2022
5. "2021 Future of Healthcare Report," HIMSS, August 2021
6. "Cost of a Data Breach Report 2022," IBM and Ponemon Institute, July 2022

Spectrum ENTERPRISE™