DekkoSecure

Securing Healthcare Data in the Digital Age

Best Practices for Protection of Shared Healthcare Data

Table of Contents

Executive Summary

The healthcare industry faces an increasing number of cyber threats, regulatory challenges, and operational inefficiencies, making the protection of sensitive healthcare data more critical than ever. Cybercriminals target healthcare organisations due to the high value of medical data on the dark web. This results in financial losses, reputational damage, and compliance risks.

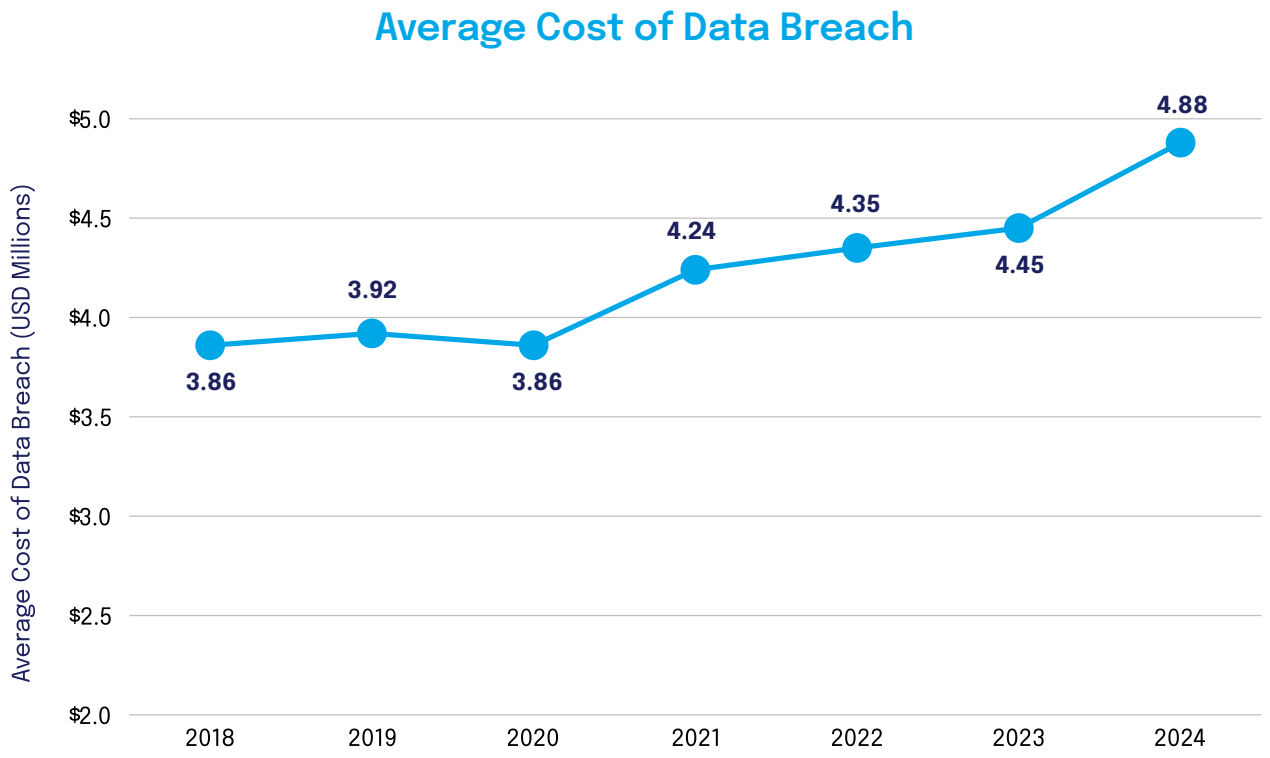
This whitepaper explores the key security challenges faced by healthcare organisations, presents best practices for mitigating security risks, and introduces DekkoSecure's unique approach to securing sensitive healthcare data.

Key Insights

- **Healthcare remains the most targeted industry for data breaches, with an average cost of USD 9.23 million per incident.** *(Ponemon Institute, 2023)*

- **Over 70% of healthcare organisations have experienced a significant security incident in the past year.** *(HIMSS Cybersecurity Survey, 2023)*

- **Insider threats account for 25% of healthcare data breaches, highlighting the need for stricter access controls.** *(Verizon Data Breach Investigations Report, 2023)*



Introduction: The Growing Threat to Healthcare Data Security

The healthcare sector is experiencing an unprecedented increase in cyber threats, driven by:

- The **high value of healthcare data** makes it lucrative for cybercriminals involved in identity theft and insurance fraud.
- **Regulatory pressures**, as governments enforce stricter data protection laws and impose harsher penalties for non-compliance.
- **Operational inefficiencies**, where outdated or partially secure file-sharing tools create vulnerabilities that lead to data breaches.

With the rapid adoption of digital health records and a significant increase in telemedicine, organisations must implement data security solutions that are **end-to-end encrypted, and that comply with Australian and international data protection regulations.**

Recent Significant Data Breaches

The Medibank Data Breach

In October 2022, Medibank, one of Australia's largest private health insurers, suffered a catastrophic cyberattack that exposed the sensitive medical records of 9.7 million current and former customers. The breach was caused by compromised login credentials obtained through an unpatched vulnerability in Medibank's network, allowing attackers to gain unauthorised access. **A critical factor in the severity of the breach was that the sensitive customer data was not encrypted, making it easily accessible once the attackers infiltrated the system.**

The Russian-linked ransomware group responsible for the attack exfiltrated highly sensitive personal data, including names, birth dates, Medicare numbers, and detailed health claims information. Medibank refused to pay the ransom, prompting the attackers to publish customer health data on the dark web. The breach had severe reputational and financial consequences, costing the company an estimated $46.4 million in remediation and response efforts (ABC News, 2022; Australian Cyber Security Centre, 2022).

Kansas City Hospital Ransomware Attack

In January 2024, multiple hospitals in Kansas City suffered a devastating ransomware attack that shut down their systems for days, leaving medical staff unable to access patient records, perform critical surgeries, or provide timely care. According to reports, cybercriminals infiltrated the hospital networks through a phishing attack, encrypting sensitive data and demanding a ransom for its release. The attack not only jeopardised patient privacy but also put lives at risk as hospitals struggled to continue operations.

The breach underscored the urgent need for robust cybersecurity measures, including secure file-sharing platforms and zero-trust architecture, to prevent unauthorised access and mitigate ransomware threats *(The Beacon-News, 2024)*.

Market Context and Challenges

The risks to healthcare data are driven by multiple factors, including the rising cost of cyber incidents and evolving attack strategies. Selected industry reports below highlight the financial and operational impact of cybersecurity threats in the healthcare sector:

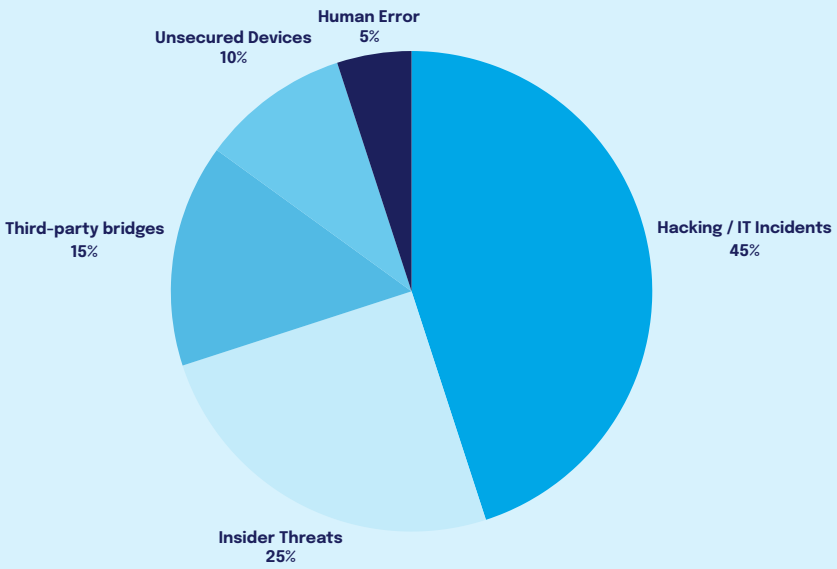
The **global average cost of a data breach** has increased by **9.66% from the previous year,** reaching USD 4.88 million.

Healthcare organisations are disproportionately affected, with **USD 9.23 million as the highest industry breach cost** *(Ponemon Institute, 2023)*.

Ransomware attacks are rising, with **34% of healthcare organisations reporting such incidents in the past year** *(HIMSS Cybersecurity Survey, 2023)*.

Insider threats account for 25% of healthcare data breaches *(Verizon Data Breach Investigations Report, 2023)*.

TOP CAUSES OF HEALTHCARE DATA BREACHES (2024)



Best Practices for Securing Shared Healthcare Data

To mitigate the risk outlined in the previous section, healthcare organisations must implement best practices that enhance security, compliance, and operational efficiency. The following measures are designed to address common cybersecurity threats and challenges.

Implement Strong Access Control Measures

- Ensure that only authorised personnel can view and share sensitive information. This helps prevent insider threats and unauthorised access to patient records.
- Apply strict authentication requirements, such as multi-factor authentication (MFA), to minimise vulnerabilities related to human error and privilege misuse.

Protect Sensitive Information at all Times

- Secure patient records and other critical data from unauthorised access by ensuring encryption **at rest, in transit, and during collaboration (E2EE)** to prevent exposure, especially when transmitting data between healthcare providers and third-party vendors.

Maintain Oversight and Accountability

- Track document access and modifications through
- real-time audit logs, addressing the lack of incident response readiness and aiding in regulatory compliance.

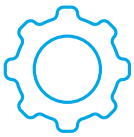
- Ensure your organisation can monitor sharing activities in real-time to detect suspicious behaviour and prevent data breaches caused by supply chain vulnerabilities.

Align Operations with Regulatory Requirements

- Avoid penalties by adhering to national privacy laws and ensuring compliance with the Australian Privacy Act and APRA CPS 234 to mitigate regulatory risks.

- Use tools that ensure data sovereignty and compliance, reducing risks associated with cross-border data transfers.

Minimise Human Error in Collaboration



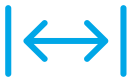
- Control access by implementing permissions that restrict file-sharing to only necessary personnel, reducing risks of insider threats and unauthorised disclosures.

- Use permission settings that align with organisational workflows to limit accidental sharing of sensitive data, addressing operational inefficiencies.

How DekkoSecure Addresses These Challenges

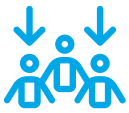
The DekkoSecure cloud-based platform provides a **government-grade secure** file-sharing and collaboration solution that meets today's healthcare security and compliance standards, **including data sovereignty**.

Key features of the platform include:



Zero-Trust Architecture

Each access request is continuously authenticated and verified. No user or device is automatically trusted, reducing the risk of unauthorised access or insider threats.



End-to-End Encryption

All files are encrypted at rest, in transit, and during collaboration. Only authorised users can access the data, preventing interception or leaks.

Zero Knowledge Security

DekkoSecure uses a zero- knowledge security model, ensuring that even DekkoSecure, the service provider, cannot access data shared on the platform. This complies with privacy regulations such as the Australian Privacy Act, restricting data visibility to authorised users only.

Granular Permission Control

Organisations are able to define precise access policies. Granular permission control ensures that users can only interact with designated files, reducing data mishandling risks.

Comprehensive Audit Trails

Every action on the platform is logged in real-time, enabling your organisation to monitor file-sharing activities for compliance and security audits. Detailed reporting supports regulatory requirements and helps detect unusual activity.

DekkoSecure Case Study: Telstra Health

Telstra Health, Australia's largest eHealth company, leverages DekkoSecure's end-to-end-encrypted platform to enhance the security of its internal file sharing and collaboration on critical projects. In the **1800RESPECT initiative** -a national service operated by Telstra Health on behalf of the Australian government that provides confidential support to individuals affected by domestic, family, and sexual violence- DekkoSecure ensures that sensitive information remains protected during communication between support teams and external partners.

Similarly, the **National Cancer Screening Register (NCSR)**, also operated by Telstra Health on behalf of the Australian government, consolidates and manages participants' screening records, and uses DekkoSecure to facilitate secure data exchange among healthcare providers, laboratories, and government entities. By integrating the capabilities of the DekkoSecure platform, Telstra Health addresses the critical need for secure, compliant, and efficient data handling across its services.

DekkoSecure Case Study:
Nexus Hospitals

Nexus Hospitals, a prominent Australian private hospital group, sought a secure and efficient solution to share sensitive patient records with external stakeholders, such as clinics, specialists, and legal representatives. Traditional methods like email and shared drives posed security risks and inefficiencies, necessitating a modern, encrypted, and structured approach to medical records management.

By implementing a **cloud-based collaboration platform**, Nexus Hospitals established a streamlined and secure workflow that accommodates both private and public record-sharing needs:

- Private Records: Access is restricted to authorised internal personnel, ensuring strict confidentiality.
- Public Records: Authorised external stakeholders can securely access necessary information, facilitating effective collaboration.

The DekkoSecure platform is utilised by various roles within the hospital group, including administrative staff, health information managers, and medical professionals, ensuring that all team members can securely manage and share patient information. External stakeholders, such as clinics, specialists, and legal representatives, also benefit from secure access to pertinent records, enhancing collaboration and patient care.

With **end-to-end encryption**, **strict access controls**, and **real-time audit trails**, Nexus Hospitals has strengthened data security, improved compliance, and streamlined record management—protecting patient confidentiality while enhancing collaboration.

DekkoSecure

Contact DekkoSecure to learn more

Contact us

Or visit our website:

www.dekkosecure.com