# Unveiling the biggest threats to privacy, cyber security, and resilience in healthcare

In an era dominated by digital technologies, the healthcare industry faces an increasing number of threats to privacy, cybersecurity, and resilience. The sensitive nature of patient data, coupled with the rapid digitisation of healthcare systems, has made the sector an attractive target for malicious actors. In this article, we will explore some of the biggest threats that pose significant risks to privacy, cybersecurity, and resilience in healthcare.

## Ransomware attacks

Ransomware attacks have become one of the most pervasive and disruptive threats to healthcare organisations. These attacks involve encrypting critical data and demanding a ransom in exchange for its release. According to recent reports, the healthcare sector has experienced a surge in ransomware incidents, leading to significant disruptions in patient care and the potential compromise of sensitive data. These attacks exploit vulnerabilities in outdated systems, human error, and inadequate security measures.

## Data breaches and unauthorised access

Data breaches and unauthorised access remain major concerns in healthcare. With the increasing interconnectedness of healthcare systems and the vast amount of patient data stored electronically, unauthorised access can lead to the exposure of highly sensitive information. Whether it's personal health records, financial data, or personally identifiable information (PII), the consequences of a data breach can be severe, including identity theft, financial fraud, and reputational damage to healthcare organisations.

## Insider threats

Insider threats pose a significant risk to the privacy and security of healthcare data. Employees, contractors, or other trusted insiders who have access to sensitive information may deliberately or inadvertently misuse or disclose patient data. Whether driven by financial gain, personal motives, or negligence, insider threats can have devastating consequences. Organisations need robust security protocols, access controls, and ongoing monitoring to mitigate the risks associated with insider threats.

## Iot and connected medical devices

The proliferation of Internet of Things (IoT) devices and connected medical devices has introduced new vulnerabilities to healthcare systems. Many of these devices lack adequate security measures, making them susceptible to cyberattacks. Compromised devices can be exploited to gain unauthorised access to networks, manipulate medical data, or disrupt critical medical equipment. The healthcare industry must address the security of IoT and connected medical devices by implementing robust security protocols, regular updates, and vulnerability assessments.

### Lack of cybersecurity awareness and training

Human error remains a significant contributor to cybersecurity breaches in healthcare. The lack of cybersecurity awareness and training among healthcare professionals increases the likelihood of falling victim to phishing attacks, social engineering, or inadvertently sharing sensitive information. Effective training programs should educate employees on recognising and responding to potential threats, employing strong passwords, and understanding the importance of cybersecurity hygiene.

### Regulatory and compliance challenges

Navigating complex regulatory frameworks and compliance requirements is a continual challenge for healthcare organisations. Compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) or the General Data Protection Regulation (GDPR) is critical to protecting patient privacy and avoiding penalties. However, keeping up with evolving regulations and ensuring compliance across the organisation can strain resources and potentially leave gaps in cybersecurity and resilience efforts.

## Addressing the threats

Protecting privacy, ensuring cybersecurity, and building resilience are paramount for the healthcare industry. The threats discussed in this article, including ransomware attacks, data breaches, insider threats, vulnerabilities in IoT and connected devices, lack of cybersecurity awareness, and compliance challenges, highlight the urgency for healthcare organisations to strengthen their security measures.

Implementing robust cybersecurity frameworks, conducting regular risk assessments, investing in employee training, and collaborating with industry stakeholders are crucial steps in safeguarding patient privacy and maintaining the integrity of healthcare systems in the face of evolving threats.

## Contact us:


**Rajvir Cheema**
**Partner, Digital Healthcare Advisory**
KPMG in the UK
**E:** rajvir.cheema@kpmg.co.uk

**Richard Krishnan**
**Partner, Technology and Cyber Risk**
KPMG in the UK
**E:** richard.krishnan@kpmg.co.uk

**Thomas Jordan**
**Cyber Senior Manager**
KPMG in the UK
**E:** thomas.jordan@kpmg.co.uk


**Find out more:** home.kpmg/uk/cyberforhealth

**kpmg.com/uk**

**Some or all of the services described herein may not be permissible for KPMG audited entities and their affiliates or related entities.**




Document Classification: KPMG Public

CREATE: CRT152957A I December 2023