Fostering behavioural change in healthcare for a more secure NHS

In an era marked by increasing cyber threats, the need for a more secure National Health Service (NHS) has become paramount. While technological advancements play a crucial role in bolstering cybersecurity, it is equally important to recognise the significance of behavioural change in creating a robust and secure healthcare environment. In this article, we will explore the behavioural changes required within healthcare to establish a more secure NHS.

Cultivating a culture of cybersecurity awareness

Developing a culture of cybersecurity awareness is fundamental to creating a more secure NHS. Healthcare professionals at all levels should be educated on the potential risks and best practices for maintaining data security and privacy. This includes raising awareness about phishing attacks, password hygiene, social engineering techniques, and the importance of regularly updating software and systems. By fostering a collective sense of responsibility for cybersecurity, healthcare workers become an essential line of defence against potential threats.

Encouraging proactive reporting of security incidents

Effective reporting of security incidents is crucial for identifying and addressing vulnerabilities promptly. Encouraging healthcare staff to report any suspicious activity, including potential breaches or attempted cyberattacks, is vital. It is essential to establish clear reporting mechanisms and ensure that reporting incidents does not carry punitive consequences. Promoting a blame-free culture empowers staff to come forward with concerns, enabling quick mitigation measures and collective learning from incidents.

Implementing robust access controls and data governance

Implementing strong access controls and data governance practices is essential for safeguarding patient information. Healthcare organisations must adopt a least-privilege approach, granting employees access only to the data necessary for their roles. Regular reviews of access privileges and swift deactivation of accounts for former employees are critical to preventing unauthorised access. Implementing data classification and encryption mechanisms further enhances data protection, ensuring that sensitive information remains secure, even in the event of a breach.

Prioritising data privacy and consent

Respecting patient privacy and obtaining informed consent are integral to creating a more secure NHS. Healthcare providers must prioritise patient privacy, ensuring that personal information is only accessed and shared as necessary for providing care. Transparent communication regarding data collection, usage, and storage practices is essential to building trust with patients. Organisations should also implement robust consent management systems that enable patients to make informed decisions about the use of their data.

Investing in ongoing training and development

Continuous training and development programs are essential for healthcare professionals to stay up to date with the evolving cybersecurity landscape. This includes educating staff on emerging threats, new regulations, and best practices for data protection. Training should also encompass practical exercises, such as simulated phishing campaigns or incident response drills, to reinforce knowledge and improve incident handling capabilities. Ongoing education ensures that healthcare professionals remain vigilant and adaptable in the face of evolving cyber threats.

Collaboration and information sharing

Collaboration and information sharing among healthcare organisations are vital for building a more secure NHS. Encouraging the exchange of best practices, threat intelligence, and lessons learned from security incidents enables healthcare organisations to collectively enhance their cybersecurity posture. Sharing anonymised data on cyber threats and attacks can help identify trends, enabling proactive measures to be taken at a national level to counter emerging threats effectively.

Securing healthcare services

Creating a more secure NHS requires a collective effort that goes beyond technology and infrastructure. By fostering behavioural change within healthcare, including cultivating cybersecurity awareness, encouraging incident reporting, implementing robust access controls and data governance, prioritising data privacy and consent, investing in ongoing training, and promoting collaboration, healthcare organisations can significantly enhance their security posture. These behavioural changes will help fortify the NHS against cyber threats, safeguard patient data, and maintain the trust and integrity of the healthcare system.

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

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

kpmg.com/uk

Document Classification: KPMG Public

CREATE: CRT152957A I January 2024