VOL.16 NO.5 PAGES 44 www.expresshealthcare.in

EXPRESS HEALTHCARE

INDIA'S FOREMOST HEALTHCARE MAGAZINE

JUNE 2023, ₹50

Interview

Jonas Muff
Founder and CEO,
Vara

Diagnostics
Dinesh Chauhan,
CEO, CORE Diagnostics

IT INFRA IN HEALTHCARE IN NEED OF SYSTEMATIC APPROACH

More investment and adoption of stringent policies are required to build secure and sustainable IT infrastructure in healthcare

EXPRESS HEALTHCARE

Chairman of the Board
Viveck Goenka

Sr. Vice President-BPD
Neil Viegas

Vice President-BPD
Harit Mohanty

Editor
Viveka Roychowdhury*

Editorial Team
Lakshmipriya Nair
Kalyani Sharma

DESIGN
Art Director
Pravin Temble

Senior Designer
Rekha Bisht

Senior Artist
Rakesh Sharma

Marketing Team
Rajesh Bhatkal
Ashish Rampure
Debnarayan Dutta

Production Co-ordinator
Dhananjay Nidre

Scheduling & Coordination
Pushkar Waralikar

CIRCULATION
Mohan Varadkar

CONTENTS

Express Healthcare®

Regd. With RNI No.MAHENG/2007/22045. Postal Regd.No.MCS/162/2022 - 24. Printed and Published by Vaidehi Thakar on behalf of The Indian Express (P) Limited and Printed at The Indian Express Press, Plot No.EL-208, TTC Industrial Area, Mahape, Navi Mumbai-400710 and Published at Mafatlal Centre, 7th floor, Ramnath Goenka Marg, Nariman Point, Mumbai 400021.

Editor: Viveka Roychowdhury.* (Editorial & Administrative Offices: Mafatlal Centre, 7th floor, Ramnath Goenka Marg, Nariman Point, Mumbai 400021)

* Responsible for selection of news under the PRB Act.

IT INFRA IN HEALTHCARE IN NEED OF SYSTEMATIC APPROACH

More investment and adoption of stringent policies are required to build secure and sustainable IT infrastructure in healthcare

By Kalyani Sharma

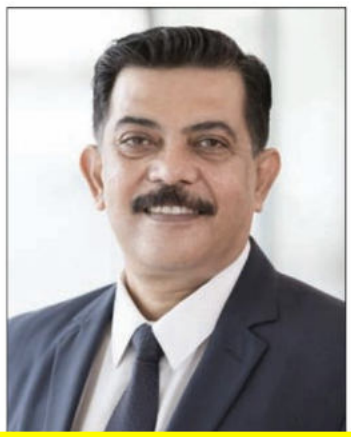
India's healthcare and hospital IT infrastructure has been undergoing significant advancements and digital transformations in recent years be it adoption of Artificial Intelligence (AI), Electronic Health Records (EHR), Health Information Exchange (HIE), telemedicine, health management information systems or mobile health apps. This had led to the healthcare IT infrastructure becoming more interconnected and data-driven. With the huge amount of health data being stored and collected, robust cybersecurity measures is the need of the hour.

The recent AIIMS cyberattacks is just one example that underlines the gaps that still need to be filled. Healthcare/Hospital IT infrastructure in our country has a lot to catch up on in terms of investment, stringent policies and other parameters.

Talking about the role of cybersecurity, Vishal Salvi, Chief Information Security Officer & Head of Cyber Security Practice, Infosys said, "Cyber-attacks in the health and life sciences sectors have surged in the aftermath of the pandemic. As the healthcare sector continues to undergo digital transformation, the risk of cyber-attacks is inevitable. In 2022 alone, the healthcare industry in India faced over 1.9 million cyberattacks, as per cybersecurity think tank CyberPeace Foundation and Autobot Infosec Private Ltd. Cybersecurity plays a crucial role for healthcare providers to build trust among people over their data. Securing the massive volumes of data that the healthcare sector possesses is only the first step. To be resilient to cyber threats, organisations need to build a highly adaptive security ecosystem which encompasses enforcing IT hygiene, building defence mechanisms, improving risk management, and managing threat detection and response. At Infosys, we enable our customers to drive a mindset built on 'secure by design' which ensures that security is deeply embedded in their systems, and not deployed as an afterthought."

A sustainable cybersecurity approach is one that takes care of today's needs and anticipates tomorrow's requirements

Vishal Salvi
Chief Information Security Officer & Head of Cyber Security Practice,
Infosys

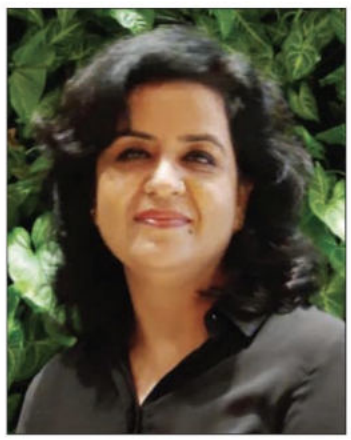


With exposure management, healthcare providers can successfully reduce cyber risk and strengthen their defences, making it more expensive for hackers to breach their organisations essentially cutting through the noise to effectively establish deterrence

Kartik Shahani
Country Manager,
Tenable India

One of the biggest challenges with patient data is that there's so much of it! And working with our clients, we see this data spread across a multitude of disparate IT systems which throws up more challenges

Vaidant Singh
Chief Marketing Officer,
SourceFuse



Connected medical devices are another area of concern for cybersecurity in Indian healthcare. Pacemakers, insulin pumps, and monitoring systems are all becoming increasingly connected to the internet, making them vulnerable to cyber-attacks

Shikha Sharma
Sr. Manager & Head IT,
PSRI Hospital

Minatee Mishra, Director, Product Security – Security Center of Excellence, Philips Innovation Campus said, "Healthcare is a lucrative market for hackers globally because of the treasure trove of sensitive data and traditionally weak security controls. The threat landscape is evolving rapidly and entry barriers for malicious attackers are low (e.g. Ransomware as a Service). The attacks on some of the reputed healthcare institutions demonstrate that we in India aren't immune to evolving threats."

Quoting some numbers, Vikram Thaploo, CEO-Telehealth, Apollo Hospitals Enterprises said, "A recent simulation conducted by CyberPeace Foundation, a cybersecurity think tank, revealed that the Indian healthcare industry faced approximately 1.9 million cyberattacks in 2022. The most recent incidents include the cyber-attack on two prominent public health facilities in Delhi, underscoring the urgent need for robust cybersecurity infrastructure in the healthcare sector."

Kartik Shahani, Country Manager, Tenable India also mentions, "The 2022 Threat Landscape Report by Tenable revealed that India's healthcare sector was the second most targeted by cybercriminals, signalling that innovation has outpaced cybersecurity due diligence within the industry. Given how the threat landscape has changed, it's never been more important for healthcare organisations to view the entire attack surface, detect the attack pathways cybercriminals could take and identify the most critical assets exposed."

Present issues that must be resolved while engaging with patient data

When engaging with patient data in India, there are

several issues that need to be addressed and resolved to ensure data privacy, security, and compliance with relevant regulations.

Vaidant Singh, Chief Marketing Officer, SourceFuse shares his experience with patient data. He explains, "One of the biggest challenges with patient data is that there's so much of it! And working with our clients, we see this data spread across a multitude of disparate IT systems which throws up more challenges: for doctors, not having a complete patient history during consultations impedes patient care; the power to extract business intelligence and track population health trends is unfeasible; for overburdened call centers, leveraging data to improve efficiencies falls by the wayside; and with so many systems in use, data security and regulatory compliance may be compromised. The solution is data aggregation, having one platform that seamlessly connects all the dots. While each client has unique objectives, data consolidation in the cloud is often the common goal, and from there the opportunities to leverage advanced and sophisticated cloud tech & services is boundless."

According to Shikha Sharma, Sr. Manager & Head IT, PSRI Hospital, connected medical devices are another area of concern for cybersecurity in Indian healthcare. Pacemakers, insulin pumps, and monitoring systems are all becoming increasingly connected to the internet, making them vulnerable to cyber-attacks. Healthcare organisations must prioritise the cybersecurity of these devices by implementing measures such as firmware updates, firewalls, and intrusion detection systems. Implementing these measures can ensure that medical devices are secure and patient safety is not compromised.

Thaploo added, "The growing reliance on IoT and software-driven medical equipment has introduced cybersecurity concerns surrounding legacy devices and systems. By implementing incentive-based programs, the medical industry can encourage the development of modular and updatable medical technology and software that adheres to minimum cybersecurity standards."

India has no comprehensive laws that protect the privacy of individuals' personal data, including health records. This leaves citizens vulnerable to data breaches and misuse of their data

Vishal Gondal
Founder & CEO,
GOQii

The collection and sharing of patient data come with ethical and legal considerations. Healthcare providers must ensure that patients' data is collected with their informed consent, stored securely, and shared only with authorised parties

Vikaas Bhatnagar
Chief Information Officer,
Asian Institute of Medical Sciences

Patients must have easy access to their own data in order to participate in their own care and make informed decisions. This requires making data available in a format that patients can understand and use

Karunya Sampath
Co-founder & CEO,
Payoda Technologies

The first step towards enhancing data security is to develop and implement a comprehensive security plan. This plan should include an assessment of the hospital's risks and vulnerabilities, as well as a detailed description of security policies, procedures, and controls

Tanay Tulsaney
Co-Founder,
DigiLantern

As per experts, data privacy and consent, data quality and its interpretation and transparency are some of the key present issues.

Discussing about the current issues, Vishal Gondal, Founder & CEO, GOQii said, "India has no comprehensive laws that protect the privacy of individuals' personal data, including health records. This leaves citizens vulnerable to data breaches and misuse of their data. Also, patients do not have control over how their data is used by healthcare providers, or who can access it. This also means that patient data can be shared with third parties without the patient's knowledge or consent, raising serious privacy concerns."

"Healthcare technology firms have to exercise significant care when collecting, processing, and storing personal health data. While sharing health data may be the key to medical innovations that transform patient care; checks and balances should be put in place, with clear guidelines on accountability before the implementation of digital healthcare across the country. Privacy settings for health records on health apps should allow the patient to either share their health records with their health coach and doctor or keep them private and visible only to themselves. The healthcare apps should let the patient using the app decide whether they want to share their future posts publicly, with just their friends, or keep them visible to only themselves", he added.

Emphasising on the issue of collection and sharing data,

Vikaas Bhatnagar, Chief Information Officer, Asian Institute of Medical Sciences said, "The collection and sharing of patient data is essential for effective healthcare delivery, research, and policymaking. However, the collection and sharing of patient data come with ethical and legal considerations. Healthcare providers must ensure that patients' data is collected with their informed consent, stored securely, and shared only with authorised parties.

"Additionally, healthcare providers must ensure that they comply with data protection laws, such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). These laws require healthcare providers to ensure the confidentiality, integrity, and availability of patient data."

Patient data must be accurate and complete in order to be useful for decision-making. This requires careful data collection and management practices.

Karunya Sampath, Co-founder & CEO, Payoda Technologies shares some steps that healthcare organisations can take to improve the quality of patient data which includes standardising data collection and coding practices, validating data for accuracy and completeness and using data quality tools to identify and correct errors.

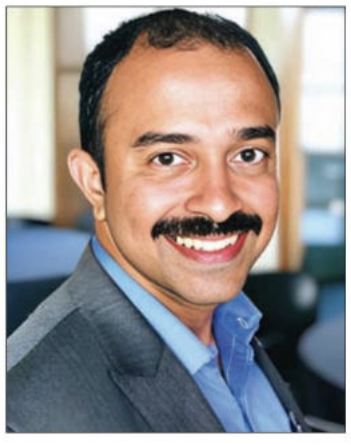
On data accessibility she explains that patients must have easy access to their own data in order to participate in their own care and make informed decisions. This requires making data available in a format that patients can understand and use. Some of the ways that healthcare organisations can make data more accessible to patients includes providing patients with online access to their EHRs, creating patient-friendly summaries of EHR data and providing patients with educational materials about their data.

One approach to safeguard hospital networks is by implementing XDR-enabled anti-virus protection, which can provide protection against virus and ransomware attacks

Karan Thakral
Vice President-IT,
CK Birla Hospital

Data privacy tools are the components that secure networks, like backup data, antivirus, data accessibility, etc. Ensure to use these tools wisely, as they could potentially help secure the entire network in the first place

Dr Sanjay Durani
Medical Superintendent,
Sanar International Hospitals



It is crucial to generate awareness within the industry about the importance of security, allocating sufficient budgets, attracting skilled professionals, and adopting strong strategic and tactical approaches to safeguard data

Manu Pathumana
Vice President,
Cyber Defense Services,
Mphasis

Monitoring IT systems, implementing incident response plans, and robust data backup and recovery plans go a long way in detecting, containing, and mitigating the impact of data breaches

Sajiv Nair
Assistant CTO and Managed services head,
ESDS software solutions

Dr Nithin Kumar, Associate Professor of Community Medicine, Kasturba Medical College, and Manipal Academy of Higher Education and Dr Partha Protim Hazarika, Assistant Professor of Health Information Management, Manipal College of Health Professions, Manipal Academy of Higher Education explains, "While handling patient data, ensuring its safeguarded storage is of utmost importance. Breaches in patient data safety can lead to unauthorised access, fraudulent incidents like identity theft, and potential harm to patients with possible consequent medico-legal complications. Similarly, caution must also be exercised in the appropriate collection and usage of the data, to ensure optimum benefits from the same. This comprehensive approach mandates smooth collaboration and cooperation amongst healthcare providers, technology vendors, administrators, policymakers, and patients."

"On data transparency they mention, "clear and transparent consent processes should be established, ensuring that patients understand how their data is collected, used, stored, and shared. Healthcare organisations and technology vendors should develop secure, user-friendly, and accessible platforms for patients to access their data in digital format."

Key measures to protect hospital data security in the public and private sector

According to the World Health Organization (WHO), up to 1 in 4 hospitals worldwide have experienced data breaches, which can result in serious consequences for patients, such as identity theft or the exposure of sensitive medical information.

Experts suggest that developing a security plan, conducting a risk assessment, data encryption, data backup and recovery, regular software updates and employee

education and training are some of the key measures that can help in protecting hospital data.

Conducting a comprehensive risk assessment helps identify potential vulnerabilities, threats, and risks to the IT infrastructure. This assessment includes evaluating systems, networks, applications, and devices to determine security gaps and establish appropriate controls.

Explaining the role of developing a security plan, Tanay Tulsaney, Co-Founder, DigiLantern, highlights, "The first step towards enhancing data security is to develop and implement a comprehensive security plan. This plan should include an assessment of the hospital's risks and vulnerabilities, as well as a detailed description of security policies, procedures, and controls. It should also outline the responsibilities of staff members and the procedures for reporting security incidents."

Karan Thakral, Vice President-IT, CK Birla Hospital shares, "One approach to safeguard hospital networks is by implementing XDR-enabled anti-virus protection, which can provide protection against virus and ransomware attacks. Hospital networks can also be protected through state-of-the-art firewalls, which are monitored and managed in real-time, with the latest threat signature updated to protect against potential cyber-attacks."

When it comes to data handling, sensitive data should be encrypted both in transit and at rest. Encryption helps protect patient information from unauthorised access and ensures that even if data is intercepted or stolen, it remains unreadable without the decryption key. Also, there should be regular implementation of regular data backup procedures to ensure data can be restored in the event of a ransomware attack, data loss, or system failure. Off-site backups and testing the restoration process are crucial to maintain data integrity.

The development of a comprehensive national health data policy, the implementation of strong data protection regulations are some of the key reforms necessary to improve India's health data security ecosystem

Dr R S Nehra
Principal Consultant,
Cyber Security,
Aakash Healthcare

Data that is sensitive to patients should be encrypted during storage, transmission, and processing to ensure their confidentiality

Gaurav Parchani
CTO & Co-founder,
Dozee

India can learn the global best practices for health data security through international engagements

Mahesh Shinde
Director - IT, P.D.
Hinduja Hospital and Medical Research Centre

The Healthcare sector should recognise the critical data elements and should plan a multiple-level data security framework to protect data

Raj Gore
CEO,
Healthcare Global Enterprises

Explaining about data privacy tools, data storage and networks, Dr Sanjay Durani, Medical Superintendent, Sanar International Hospitals said, "The network should be private and secured through a firewall and access policies. Data privacy tools are the components that secure networks, like backup data, antivirus, data accessibility, etc. Ensure to use these tools wisely, as they could potentially help secure the entire network in the first place. If our data privacy tools are robust, such threats are less likely. As far as data storage is concerned, every patient's data is essential in their patient journey; doctors need to go through already collected data and set the direction of treatment. Hence, it should be secured and maintained correctly in the first place. Even if systems crash, the organisation will have backup data for treatment while the entire system is in recovery mode."

Shahani emphasises on the role of exposure management in protecting data. He said, "Any cybersecurity professional in the healthcare industry would know that sensitive patient data is a big draw for financially motivated cybercriminals. Not only is that data valuable to the organisation, but it is critical for quality patient care and, frequently, lives depend on it remaining secure and available at all times. With exposure management, healthcare providers can successfully reduce cyber risk and strengthen their defences, making it more expensive for hackers to breach their organisations — essentially cutting through the noise to effectively establish deterrence."

Gaurav Parchani, CTO & Co-founder, Dozee while talking about access Control and authentication mentions, "Data that is sensitive to patients should be encrypted during storage, transmission, and processing to ensure their

confidentiality. Restrict unauthorised access to patient information by using strong access controls, such as role-based access, multi-factor authentication, and privileged access management."

Employees should be aware of the importance of safeguarding patient data and understand their role in maintaining cybersecurity. Their training and educating them about cybersecurity and best practices, such as identifying phishing emails, using strong passwords, and reporting suspicious activities can go a long way in preventing such threats.

On this, Manu Pathumana, Vice President, Cyber Defense Services, Mphasis stresses, "As the healthcare industry undergoes digital transformation to meet the increasing demand for services, protecting data becomes paramount for both public and private sectors. Weak security postures, often resulting from overlooking security as an afterthought, can lead to breaches and incidents. It is crucial to generate awareness within the industry about the importance of security, allocating sufficient budgets, attracting skilled professionals, and adopting strong strategic and tactical approaches to safeguard data."

Sajiv Nair, Assistant CTO and Managed services head ESDS software solutions also highlight, "Monitoring IT systems, implementing incident response plans, and robust data backup and recovery plans go a long way in detecting, containing, and mitigating the impact of data breaches. There is, however, more to be done, as employees play a crucial role in maintaining cyber resilience. Employing a culture of digital hygiene amongst the workers and equipping them with the skills and knowledge to identify and respond to potential attacks is equally essential."

Cyber risk quantification involves assessing and measuring the potential impact of cyber threats and attacks on an organisation's finances and operations. By quantifying cyber risks, hospitals can prioritise investments in cybersecurity and digital transformation based on their potential impact on the hospitals

Rahul Tyagi
Co-Founder, SAFE India

The growing reliance on IoT and software-driven medical equipment has introduced cybersecurity concerns surrounding legacy devices and systems

Vikram Thaploo
CEO-Telehealth,
Apollo Hospitals Enterprises

Healthcare is a lucrative market for hackers globally because of the treasure trove of sensitive data and traditionally weak security controls.

Minatee Mishra
Director,
Product Security – Security Center of Excellence,
Philips Innovation Campus

Governance and policy reforms necessary to improve India's health data security ecosystem

Improving India's health data security ecosystem requires governance and policy reforms to address existing gaps and strengthen data protection measures.

India is already in the process of enacting the Personal Data Protection Bill (PDPB), which aims to establish comprehensive data protection laws. The bill once passed should be implemented effectively, providing a clear legal framework for the protection of health data, defining rights and obligations, and establishing penalties for non-compliance.

Tulsaney said, "India has made notable advancements in its healthcare sector, but it is crucial to prioritise governance and policy reforms for the safety and privacy of healthcare data. The WHO provides a useful guideline for governments to establish robust health data governance frameworks, implement data protection policies, and invest in secure technical infrastructure. Implementing these measures would help India build a robust health data security ecosystem and take significant strides toward safeguarding patient and healthcare provider information."

According to Dr R S Nehra, Principal Consultant, Cyber Security, Aakash Healthcare, "The development of a comprehensive national health data policy, the implementation of strong data protection regulations, promotion of interoperability standards, strengthening of cybersecurity infrastructure, and promotion of public-private partnerships are some of the key reforms necessary to improve India's health data security ecosystem. While the Personal Data Protection Bill, 2019, is a step in the right direction, but it needs to be implemented with strict regulations and penalties for non-compliance."

Fostering collaboration between the government, healthcare industry, and technology providers to jointly address data security challenges is also important as it can leverage the expertise and resources of both sectors to develop innovative solutions and frameworks for health data protection.

Another important aspect is conducting public awareness campaigns to educate individuals about their rights regarding health data privacy and the importance of secure data handling. Empowering individuals with knowledge will enable them to make informed decisions and actively participate in protecting their own health data.

Raj Gore, CEO, Healthcare Global Enterprises also highlights, "Cybersecurity plays a critical role in protecting sensitive patient information, maintaining uninterrupted healthcare services, and meeting regulatory requirements. It secures data from unauthorised access, breaches, and data theft, ensuring confidentiality. The Healthcare sector should recognise the critical data elements and should plan a multiple-level data security framework to protect data. This is best done if we refer and follow standards like ISO 27000-2022 and HIPAA. The Government of India should pass a proper Data Protection and Privacy Law. In the absence of the same. We are following what is best references available outside the country. The issue with doing so is that there are many items/clauses which are to be dealt with differently in our country-specific context. The

field of cybersecurity requires continuous effort, with organisations needing to consistently enhance their security measures in response to ever-changing threats."

Stressed hospital budgets and digital transformation

In the context of stressed hospital budgets, making a compelling case for digital transformation in India's healthcare sector requires highlighting the benefits beyond data security.

In this context, Salvi explains, "Amid changing demographics of customers with sophisticated expectations as well as increased regulatory scrutiny, digital transformation is inevitable. By capitalising on digital technologies such as AI and cloud computing, healthcare organisations can aim to provide more accessible, affordable, intelligent, and accurate services. In addition to data security, a well-designed security system can also predict and slow down attacks, while preventing damage before it occurs."

"A sustainable cybersecurity approach is one that takes care of today's needs and anticipates tomorrow's requirements. Given the dynamic nature of the current business environment and economic climate, ignoring building future capabilities could cost one in the long run."

Dr Kumar and Dr Hazarika shares, "When advocating for digital transformation in a hospital with a limited budget, we must keep in mind that, while making the initial investment in digital technologies may appear intimidating, it is critical to consider the long-term cost-saving potential and value that digital transformation can bring to healthcare organisations. By demonstrating how digital transformation can optimise operations, improve patient outcomes, and generate cost savings, healthcare organisations can make a compelling case for prioritising digital initiatives despite budget constraints.

Pathumana stresses, "With the daunting challenge of meeting the high demand for healthcare services amid limited resources, the imperative for digital transformation in the healthcare industry cannot be overstated. Waiting for extensive physical infrastructure and a substantial increase in healthcare professionals is simply not feasible given the urgency of the situation. In this context, digital transformation serves as a powerful force multiplier, enabling us to leverage existing resources and facilities to reach a larger segment of the urban and rural population in need of quality healthcare services."

"The benefits of digital transformation extend far beyond mere data security. It presents hospitals with an expanded addressable market, promising improved return on investments, revenue growth, enhanced access to talent, and staff development opportunities. By embracing digital solutions, healthcare institutions can also contribute significantly to larger national and societal goals of equitable healthcare access. However, it is crucial to recognise that successful digital transformation relies heavily on robust cybersecurity measures. Protecting patient data and ensuring privacy are paramount for fostering trust and maintaining the integrity of healthcare systems."

By emphasising on the number of benefits and showcasing how digital transformation can address budget constraints while delivering improved patient care and long-term cost savings, India's healthcare sector can make a strong case for embracing digital technologies and securing the necessary funding and support for implementation.

Rahul Tyagi, Co-Founder, SAFE India opines that cyber risk quantification is one way to make a case for digital transformation despite stressed hospital budgets stresses. He explains that cyber risk quantification involves assessing and measuring the potential impact of cyber threats and attacks on an organisation's finances and operations. By quantifying cyber risks, hospitals can prioritise investments in cybersecurity and digital transformation based on their potential impact on the hospitals. In addition to improving data security, digital transformation can bring other benefits to hospitals, such as increased efficiency, improved patient care, and reduced costs. For example, digital health solutions like telemedicine and remote patient monitoring can help hospitals provide care to more patients while reducing the need for physical infrastructure and staff. By quantifying the potential financial and operational impact of cyber threats and attacks, hospitals can better understand the ROI of digital transformation and make more informed investment decisions.

Way forward

Investment in IT infrastructure, adoption of stringent policies and standards, and implementation of effective cybersecurity measures are important to ensure that patient data is secure. The healthcare industry in India has a long way to go in terms of cybersecurity, but with concerted efforts, it is possible to overcome the challenges and ensure sustainable future for the industry.

Kalyani.sharma@expressindia.com
journokalyani@gmail.com

Policy reforms

- **Creation of a regulatory body:** The regulatory body should be empowered with adequate authority and resources to enforce compliance. Regular audits and inspections should be conducted to ensure that these organisations handling health data adhere to prescribed security standards
- **Data Protection Legislation:** India needs comprehensive data protection legislation that specifically addresses health data security. The legislation should establish clear guidelines on data collection, storage, processing, sharing, provisions for consent and breach notification etc.
- **Collaboration:** Collaboration between the government, healthcare industry, technology providers and research institutions are vital in today's information era. Collaboration leads to development of innovative solutions. ABDM is one example. India can learn the global best practices for health data security through international engagements.

Governance

- **Incident management system:** Establishing a robust incident response system is critical for managing data breaches effectively. Organisations should have well-defined procedures in place for detecting and reporting of breaches.
- **Continuous monitoring:** Regular monitoring and evaluation of the health data ecosystem is essential to identify the gaps, assess the effectiveness of policies and regulations and make necessary improvements.
- **Access control and authentication:** Implementing robust access control mechanisms is vital to protect health data. Two-factor authentication, strong passwords, and biometric identification can help ensure authorised access.

Source: Mahesh Shinde, Director - IT, P.D. Hinduja Hospital and Medical Research Centre

Employees should be aware of the importance of safeguarding patient data and understand their role in maintaining cybersecurity. Their training and educating them about cybersecurity and best practices, such as identifying phishing emails, using strong passwords, and reporting suspicious activities can go a long way in preventing such threats