Office of the Principal Scientific Adviser
to the Government of India

Digital Personal Data Protection (DPDP) Act, Cybersecurity, and Real-World Practices for Healthcare

RICH
Research and Innovation
Circle of Hyderabad

Research and Innovation Circle of Hyderabad

Contents

Introduction

Aana Crop Solutions provides end-to-end support for rice farming, offering rice seedlings to farmers, aggregating farm mechanization services, and facilitating paddy collection and rice sales to premium markets. The startup also promotes agri-business entrepreneurship among youth through a franchise-based model and engages in R&D focused on sustainable rice farming and reducing greenhouse gas emissions. While the approach is built on existing agricultural practices, Aana Crop Solutions differentiates itself through its integrated, scalable, and impact-driven execution model.

Opening Remarks and Welcome Addresses

The workshop commenced with introductory remarks that outlined the importance of data privacy and cybersecurity in healthcare. The opening remarks emphasized the rising threats to digital health data, the need for robust data governance, and the role of regulations in protecting patient information.

Speakers

Opening Remarks – Ms. Rashmi Pimpale - CEO, Research and Innovation Circle of Hyderabad (RICH)

Ms. Rashmi Pimpale welcomed the participants, emphasizing the significance of AI-driven innovation and responsible data governance in the healthcare sector. She highlighted the AI Research and Collaboration Network (AIRCN), an initiative under the Telangana AI Roadmap Policy, aimed at fostering interdisciplinary research, industry partnerships, and real-world AI applications.

She outlined Telangana's vision to become a global hub for AI innovation, driven by the Telangana AI Advisory Council, which integrates government, academia, and industry efforts. As the nodal agency for AIRCN, RICH is actively collaborating with leading institutions such as International Institute of Information Technology (IIIT Hyderabad), Indian Institute of Technology (IIT) Hyderabad, Indian School of Business (ISB), Birla Institute of Technology & Science (BITS) Hyderabad, National Institute of Technology (NIT) Warangal, and NALSAR University of Law, Hyderabad to develop AI-led solutions for healthcare, agriculture, and smart cities.

Ms. Rashmi Pimpale emphasized the importance of ethical AI adoption, indigenous data development, and investment in AI-driven healthcare solutions. She noted that the workshop was an outcome of a recent AI in Healthcare roundtable, reinforcing the need for robust data governance and cybersecurity frameworks. She encouraged participants to engage actively, explore collaborations, and contribute to building a secure, ethical, and innovation-driven healthcare ecosystem.

Office of the Principal Scientific Adviser to the Government of India
Workshop on
DPDP Act, Cybersecurity & Real-World Practices fo
Opening Remarks
SPEAKER
MS RASHMI PIMPALE

Ms. Rashmi Pimpale - CEO, Research and Innovation Circle of Hyderabad (RICH)

Welcome Address – Prof. P J Narayanan - Director, IIIT Hyderabad

Prof. P J Narayanan welcomed all participants to the workshop, emphasizing the growing significance of AI and data-driven technologies in shaping the future of healthcare. He highlighted how Hyderabad has emerged as a major hub for AI research and innovation, with institutions like IIIT Hyderabad playing a key role in advancing AI applications.

He acknowledged the Government of Telangana's commitment to AI-driven initiatives, referencing the establishment of AI Research & Collaboration Network (AIRCN) to foster collaboration between academia, industry, and policymakers. However, he cautioned that as AI adoption accelerates, ensuring responsible and ethical data usage becomes crucial.

Sharing an insightful example, he illustrated how even without explicit healthcare records, simple location data can reveal personal medical details, underscoring the importance of strong data governance frameworks. He stressed that while AI presents incredible opportunities, its potential risks demand careful regulation and responsible implementation.

Prof. P J Narayanan commended the workshop's focus on bridging the gap between technology, law, and policy. He emphasized the need for cross-sector collaboration to develop effective, ethical, and secure AI-driven solutions in healthcare. He encouraged participants to actively engage in discussions and explore ways to balance innovation with data protection, ensuring that AI continues to serve society while safeguarding individual privacy.

He concluded by expressing gratitude to the organizers, speakers, and attendees and reaffirmed IIIT Hyderabad's commitment to supporting interdisciplinary initiatives that advance AI innovation while upholding ethical and legal standards.

Prof. P J Narayanan - Director, IIIT Hyderabad

Special Address – Prof. Srikrishna Deva Rao - Vice Chancellor, NALSAR University of Law

Prof. Srikrishna Deva Rao delivered a compelling special address, highlighting the critical challenges facing the healthcare sector in the digital era. He emphasized that data privacy and security have become pressing concerns, especially as healthcare institutions increasingly rely on digital records and AI-driven technologies.

He underscored the rising cybersecurity threats in healthcare, pointing out that medical records contain highly sensitive personal and financial information, making them a prime target for cybercriminals. The growing number of data breaches and ransomware attacks underscores the urgent need for stronger security measures and compliance frameworks.

Prof. Srikrishna Deva Rao stressed that privacy and security must be embedded into healthcare systems from the outset, rather than being treated as afterthoughts. He emphasized the importance of fostering a culture of data ethics, where institutions and practitioners internalize the principles of the DPDP Act to ensure responsible data handling.

Acknowledging the complex regulatory landscape, he called for greater collaboration between legal experts, policymakers, cybersecurity professionals, and healthcare providers to establish robust governance structures that safeguard data integrity and patient rights.

Discussing the role of AI in healthcare, Prof. Srikrishna Deva Rao recognized its potential to revolutionize diagnostics, treatment planning, and patient management. However, he cautioned that large datasets, often required for AI efficiency, introduce concerns around liability and accountability—especially when AI systems generate incorrect or biased recommendations. He stressed that regulations like the DPDP Act are crucial in defining clear responsibility frameworks to protect patient safety.

Addressing the issue of bias in AI, he noted that poorly trained models can lead to inaccurate, unfair, or even harmful medical advice, reinforcing the need for transparent, ethical AI development. To promote responsible AI adoption, Prof. Srikrishna Deva Rao introduced NALSAR's AI Leap initiative, a program designed to set transparency standards and enhance data governance frameworks in collaboration with Web Nyay, a startup focused on ethical AI governance.

He concluded by calling for a united effort across sectors to establish data protection and cybersecurity as core principles in the healthcare ecosystem. He encouraged stakeholders to embrace a multidisciplinary approach, ensuring that AI innovation and digital healthcare progress responsibly, ethically, and securely.

Prof. Srikrishna Deva Rao - Vice Chancellor, NALSAR University of Law

Special Address – Shri T. Ravi Kiran, Commissioner, Electronic Service Delivery (MeeSeva), Department of IT, Electronics & Communications, Telangana

Shri T. Ravi Kiran delivered an address on the significance of data governance in the public sector, highlighting the vast datasets managed by the government and the critical responsibility of ensuring their ethical and secure usage. He emphasized that data, when utilized appropriately, can drive innovation, enhance service delivery, and improve governance efficiency. However, he cautioned that misuse or inadequate protection of data could lead to serious privacy concerns—a challenge that the DPDP Act directly addresses.

He outlined the government's commitment to leveraging data responsibly, stating that the Data Analytics Wing of MeeSeva would collaborate with research and academic institutions to identify practical use cases that optimize government revenue, reduce costs, and enhance public service delivery. These collaborations would focus on harnessing data insights while ensuring compliance with privacy regulations and ethical data handling.

To further strengthen AI adoption and responsible data governance, Shri Ravi Kiran introduced the concept of State AI team, which is working across various government departments and industry sectors. This team will identify AI-driven solutions tailored to the needs of Telangana's governance framework, ensuring that AI technologies are deployed effectively, securely, and for the greater public good.

He concluded by reaffirming the government's commitment to fostering a robust digital ecosystem, where innovation, security, and ethical data usage go hand in hand. He encouraged continued collaboration between policymakers, researchers, and industry leaders to ensure that Telangana remains at the forefront of AI-driven governance and data security.

Shri T. Ravi Kiran, Commissioner, Electronic Service Delivery (MeeSeva), Department of IT, Electronics & Communications, Telangana

Session 1: The DPDP Act - Key Provisions and Implications for Hospitals

Speaker: Dr. KVK Santhy, Professor, NALSAR University of Law, Hyderabad
Dr. KVK Santhy provided a comprehensive analysis of the DPDP Act and its implications for healthcare institutions, emphasizing the urgent need for stringent data protection frameworks in the wake of rapid digitization in the healthcare sector.

Key Discussion Points:

1. Consequences of Data Breaches

Dr. Santhy highlighted that digitized health data contains sensitive personal, financial, and medical information, making it highly vulnerable to cyberattacks. A data breach can have severe consequences, including identity theft, financial fraud, loss of medical history, and reputational damage for hospitals.

2. Notable Healthcare Data Breaches- Several high-profile breaches in India and globally were discussed, including:

- HealthifyMe (2021) – A hacking incident exposed health and dietary data of 1.5 million users.
- Manipal Hospitals Breach (2019) – An insider threat led to unauthorized access to patient records, resulting in data misuse and legal ramifications.
- Regal Medical Group (2022) – A cyberattack compromised patient names, Social Security numbers, and treatment records.
- Kerala Hospital Data Breach – A multi-specialty hospital in Kerala suffered a breach where test results, scans, and prescriptions from the last five years were exposed online.

3. Causes of Data Breaches

Data breaches in healthcare occur due to multiple factors, including:

- **Technical vulnerabilities** – Weak encryption, outdated systems, and software loopholes.

- **Third-party failures** – Lack of cybersecurity measures among vendors and outsourced IT services.
- Lost or stolen devices – Laptops, hard drives, and mobile devices containing patient data being misplaced or stolen.
- **Human error** – Employee negligence, weak password policies, and mishandling of patient records.
- **Malicious insider threats** – Employees or contractors intentionally misusing patient data.

4. Loopholes in the DPDP Act

While the DPDP Act mandates compensation for data breaches, it does not specify compensation for patients whose data has been compromised. This raises concerns about patient rights and accountability, necessitating further legal refinement.

5. DISHA vs. DPDP Act

Dr. Santhy highlighted that the Digital Information Security in Healthcare Act (DISHA) was originally proposed to standardize healthcare data security but has now been overshadowed by the DPDP Act. While DISHA focused specifically on health data, the DPDP Act is broader, covering all personal data but lacking the sector-specific safeguards originally envisioned for healthcare.

6. OECD Guidelines for Healthcare Data Governance

Referencing global best practices, Dr. Santhy emphasized the importance of adopting OECD principles, including:

- **Informed consent** – Patients must clearly understand how their data is collected and used.
- **Data quality** – Healthcare data must be accurate, up-to-date, and verified.
- **Purpose limitation** – Data should be collected only for specific medical or research purposes, preventing unauthorized usage.

7. DPDP Act and Healthcare Compliance

Dr. Santhy broke down the key healthcare-specific elements of the DPDP Act:

- **Explicit Consent** – Data collection should be voluntary, revocable, and informed.
- **Security Measures** – Hospitals must implement mandatory cybersecurity protections to safeguard patient data.
- **Patient Rights** – Patients have the right to access, correct, and be informed about the usage of their personal data.
- **Cross-Border Data Processing** – The DPDP Act regulates personal data processed outside India, ensuring that Indian citizen data is protected even when stored in foreign servers.

Conclusion and Key Takeaways:

Dr. Santhy concluded by reiterating that as digital transformation accelerates in healthcare, strong legal frameworks, ethical data handling, and cybersecurity measures must be prioritized. She urged healthcare institutions to:

- Adopt best practices in data security, compliance, and patient rights.
- Ensure continuous monitoring and protection against cyber threats.
- Advocate for amendments in the DPDP Act to better protect patient interests.
- Engage in cross-sector collaborations to build a secure and privacy-compliant healthcare ecosystem.

The session set the stage for deeper discussions on cybersecurity, global regulations, and real-world implementation challenges in subsequent sessions.

causes of data breach in Health Care
Root causes of data breach in healthcare organizations
Technical systems glitch (31%)
Third-party snafu (35%)
Unintentional employee action (40%)
Criminal attack (43%)

Dr. KVK Santhy, Professor, NALSAR University of Law, Hyderabad

Session 2: Data Governance and Sharing Practices in Healthcare - Hospital Perspective

Speaker: Mr. Venkat Peri, Chief Data Science and AI Officer, LV Prasad Eye Institute & Founder, CognitiveCare

Mr. Venkat Peri delivered a session on effective data governance in healthcare, emphasizing the importance of structured data management, ownership clarity, and security frameworks. His discussion revolved around the challenges in handling patient data, the risks of mismanagement, and best practices for ensuring compliance with data protection laws like the DPDP Act.

Key Discussion Points:

1. The Value of Healthcare Data & Associated Risks

- Healthcare data is highly sensitive and valuable, making it a prime target for cybercriminals.
- Lack of structured data governance in hospitals often leads to poor data quality, security vulnerabilities, and inefficiencies in patient care.
- The cost of a single patient's entire medical history in the black market is extremely high, underscoring the need for strong data protection measures.

2. Governing Healthcare Data Effectively

- **Data as an Independent Asset** – Institutions must separate storage and access mechanisms to prevent unauthorized breaches.
- **Ownership Clarity** – There should be clear policies on who owns patient data—the hospital, the patient, or a third-party vendor.
- **Classification of Data** – Categorizing data into Public, Internal, Confidential, and Sensitive helps define access control policies.

3. Data Classification Framework

- **Public Data** – Information accessible to anyone, such as published reports and research findings.
- **Internal Data** – Hospital-specific operational data, which should remain within the organization.
- **Confidential Data** – Patient medical records, billing details, and personally identifiable information (PII).
- **Sensitive Data** – Highly protected information such as genomic data, biometric details, and AI-generated patient insights.

4. Access Control & Security Measures

- **Role-Based Access Control (RBAC)** – Data access should be restricted based on predefined roles (e.g., doctors, administrators, IT staff).
- **Data Access Requests** – A formal approval process must be implemented for granting temporary or permanent access to patient records.
- **Monitoring & Audit Logging** – Hospitals should maintain detailed access logs and conduct regular audits to track and prevent unauthorized access.

5. Data Retention & Compliance

- **Data Minimization** – Healthcare providers must store only necessary data and delete outdated records to reduce security risks.
- **Incident Response Plans** – Institutions must be prepared for data breaches with predefined escalation protocols and recovery mechanisms.
- **Global Regulatory Compliance** – Hospitals should align their data governance strategies with GDPR, HIPAA, and DPDP Act requirements.

Conclusion & Key Takeaways:

Mr. Venkat Peri emphasized that effective data governance is critical for improving healthcare operations, enhancing patient trust, and ensuring regulatory compliance. He urged hospitals to:

- Prioritize data security by implementing robust encryption, access control, and monitoring systems.
- Clearly define data ownership and establish transparent governance policies.
- Conduct regular compliance checks to stay aligned with national and international data protection regulations.
- Integrate AI-driven insights responsibly while ensuring ethical data usage and bias mitigation.

His session provided valuable insights into how healthcare institutions can strengthen data governance, setting the stage for further discussions on international best practices and cybersecurity challenges.

Office of the Principal Scientific Adviser to the Government of India
RICH
Research and Innovation Circle of Hyderabad
DEEP TECH

Mr. Venkat Peri, Chief Data Science and AI Officer, LV Prasad Eye Institute & Founder, CognitiveCare

Session 3: Global Best Practices in Healthcare Data Regulation - Research Perspective

Speaker 1

Prof. Aakansha, Assistant Professor, HSRC, IIIT Hyderabad
Prof. Aakansha provided a global perspective on data privacy, examining the complexities of healthcare data governance and the challenges in ensuring compliance, security, and ethical AI integration. She discussed how different nations approach data regulation, the ongoing struggle to balance innovation with privacy protection, and the emerging challenges posed by AI in healthcare.

Key Discussion Points:

1. Who Owns Healthcare Data?

- The ownership of data varies based on jurisdiction and use case—it can be controlled by governments (state-owned datasets), private entities (market-driven AI models), or individuals (patient-owned records).
- The lack of a global standard for data ownership leads to disparities in patient rights, data access policies, and regulatory enforcement.

2. Structural Challenges in Healthcare Data Governance

- **Data Collection Issues** – Fragmented data sources, inconsistencies in electronic health records (EHRs), and lack of interoperability create inefficiencies in data sharing.
- **Data Processing Risks** – Privacy violations, AI biases, and unclear legal frameworks lead to ethical concerns, particularly in cross-border data transfers.
- **Data Deployment Challenges** – Algorithmic reliability is a major issue, as poorly trained AI models can lead to incorrect medical recommendations or reinforce systemic biases.

3. Functional Challenges in Digital Healthcare Systems

- **Data Entry Errors** – Lack of digital literacy among healthcare staff results in incorrect patient records, misdiagnoses, and medical errors.
- **Health Data Breaches** – Insufficient data protection policies and inconsistent cybersecurity measures lead to large-scale leaks of patient information, which can be exploited for discriminatory practices (e.g., insurance risk profiling).

4. Global Challenges in Data Regulation

- **Defining Sensitive vs. Non-Sensitive Data** – Different countries have varied definitions of what constitutes sensitive personal data, leading to compliance difficulties for global healthcare providers.
- **Balancing Innovation and Regulation** – Over-regulation may stifle AI advancements, while insufficient regulation increases risks related to data misuse and patient harm.
- **Ethical & Legal Concerns** – Issues like postmortem data privacy, data portability rights, and algorithmic decision-making transparency need clearer policies and enforcement mechanisms.

Conclusion & Key Takeaways:

Prof. Aakansha emphasized that while AI and digital healthcare offer transformative benefits, they also introduce complex regulatory and ethical challenges. She urged policymakers, researchers, and industry leaders to:

- Develop harmonized global data standards to ensure cross-border data protection and compliance.
- Enhance transparency in AI-driven healthcare decisions to reduce biases and improve accountability.
- Promote ethical AI adoption by integrating privacy-by-design principles into healthcare technologies.
- Address digital literacy gaps to ensure accurate data collection and secure patient records.

Her session provided valuable insights into the evolving global regulatory landscape, reinforcing the need for a balanced approach that protects patient privacy without hindering innovation.

on DPDP Act, Cybersecurity, and Real World Practices for Healthcare
ession 2: International
erspectives on ata
Privacy
st Practices in Healthcare Data Regula arch Perspective
kansha Natani/ IIIT-

Prof. Aakansha, Assistant Professor, HSRC, IIIT Hyderabad

Speaker 2

Dr. Krishna Ravi Srinivas - Adjunct Professor of Law & Co-ord CoE in AI & Law - NALSAR University of Law, Hyderabad

Dr. Krishna Ravi Srinivas provided a comprehensive overview of global healthcare data governance frameworks, focusing on the complexities of cross-border data flows, data localization policies, and regulatory compliance. His session emphasized the challenges faced by healthcare institutions in navigating fragmented international regulations and the need for a harmonized approach to data governance, particularly in the context of AI-driven healthcare systems.

Key Discussion Points:

1. The Growing Importance of Data Governance

- With exponential growth in digital healthcare data, regulatory compliance is becoming increasingly complex.
- Data localization norms are gaining traction, with governments mandating that health and financial data be stored within national borders to prevent external access.
- The European Union’s approach to data sovereignty restricts companies from storing or transferring data outside of the EU, creating challenges for international research collaborations.

2. Challenges in Cross-Border Data Flows

- No universal framework exists for regulating cross-border healthcare data transfers, leading to fragmented compliance requirements.
- Trade agreements, such as regional pacts in the UK, EU, and ASEAN, impose country-specific restrictions, making it difficult for global healthcare providers and AI companies to navigate compliance.
- Research and innovation suffer due to strict localization laws, as there are no clear exceptions for data-sharing in scientific collaborations.

3. Global Trends in Data Protection Regulations

GDPR (Europe):

- Treats health data as a special category, requiring explicit consent for collection and processing.
- Enforces strict penalties for non-compliance, including mandatory breach notifications within 72 hours.

HIPAA (United States):

- Focuses on protected health information (PHI) and mandates secure handling of electronic health records.
- Requires security safeguards but allows more flexible data sharing for research and treatment purposes.

DPDP Act (India):

- Lacks sector-specific regulations for healthcare, raising concerns over the extent of protection for medical data.
- The absence of clear guidelines on cross-border data sharing creates uncertainties for Indian healthcare institutions.

4. Data Localization and Its Implications

- Countries are increasingly enforcing local storage requirements, with some mandating that data be stored exclusively within national borders (China, Russia).
- The trade-off between security and innovation was discussed, as excessive data localization can hinder global research collaborations and AI development.
- Some nations, like Singapore, follow a hybrid model, allowing cross-border data transfers under strict regulatory oversight.

5. AI and Data Protection – Emerging Challenges

- AI models require vast amounts of healthcare data, but privacy concerns arise when AI infers medical conditions from seemingly non-sensitive data (e.g., location tracking).
- The principle of 'Minimum Necessary Use' should be enforced to ensure that only essential data is processed, reducing risks of privacy breaches.
- Liability issues in AI-based healthcare systems need to be clearly addressed, particularly when AI makes incorrect or biased medical recommendations.

6. The Role of the Data Protection Board of India (DPB)

- The DPB is tasked with enforcing the DPDP Act, but its role in monitoring healthcare data remains undefined.
- Healthcare institutions must take proactive steps to strengthen compliance, such as:
  - Implementing privacy-by-design frameworks
  - Conducting regular data impact assessments
  - Ensuring transparency in AI-driven decision-making

Conclusion & Key Takeaways:

Dr. Krishna Ravi Srinivas emphasized that India must develop a healthcare-specific data governance framework that aligns with global best practices while addressing local challenges. He urged stakeholders to:

- Advocate for amendments in the DPDP Act to include clear regulations for healthcare data protection.
- Develop standardized guidelines for cross-border healthcare data transfers to enable secure global research collaborations.
- Adopt AI ethics frameworks to prevent bias and unfair decision-making in AI-driven healthcare systems.
- Strengthen compliance mechanisms to enhance enforcement of patient data rights and minimize legal ambiguities.

His session provided valuable insights into the evolving landscape of global data protection laws, reinforcing the need for a structured and well-defined approach to healthcare data security in India.

Dr. Krishna Ravi Srinivas - Adjunct Professor of Law & Co-ord CoE in AI & Law - NALSAR University of Law, Hyderabad

Session 4: Cybersecurity Challenges in Hospitals: Protecting Patient Data & Case Studies - Research Perspective

Speaker : Mr. Irfan, Cybersecurity Analyst, CLFS, NALSAR University of Law

Mr. Irfan delivered an intensive session on cybersecurity vulnerabilities in healthcare, highlighting how hospitals are prime targets for cyberattacks due to their critical infrastructure and vast amounts of sensitive patient data. He demonstrated real-time cyber threat monitoring tools, provided case studies of recent hospital cyberattacks, and discussed actionable steps for hospitals to secure their systems.

Key Discussion Points:

1. Cybersecurity Challenges in Healthcare – The Growing Threat

- Hospitals use a wide range of connected devices, including CCTVs, biometric scanners, routers, MRI machines, and hospital management systems, many of which lack proper security measures.
- Cybercriminals target these weak entry points to steal, manipulate, or disrupt patient data and hospital operations.
- Cyber Threat Intelligence (CTI) is crucial for identifying vulnerabilities, preventing intrusions, and securing digital healthcare systems.

2. Understanding the Scale of Cyber Threats – Live Demonstration

- A live Cyber Threat Map showed that over 52,000 attacks had already occurred that day, with education, telecommunications, and government sectors being the most targeted.
- Three primary types of cyberattacks affecting hospitals:
  - **Phishing attacks** – Cybercriminals trick hospital staff into sharing sensitive information via fake emails.
  - **Malware infections** – Malicious software can encrypt or steal hospital data, disrupting operations.
  - **Ransomware attacks** – Hackers hold hospital data hostage until a ransom is paid, affecting patient care.

3. Case Study: AIIMS Cyberattack – A National Wake-Up Call

- The AIIMS (All India Institute of Medical Sciences) ransomware attack was one of the most severe cyberattacks on Indian healthcare.
- **Consequences:**
  - Hospital systems were crippled for nearly a month.
  - Patient records were encrypted, and access was blocked by hackers.
  - The hospital had to revert to manual operations for over a week, impacting patient care.

4. The Role of Advanced Persistent Threat (APT) Groups & Threat Actors

- APT groups are highly sophisticated hacking collectives
- Hackers infiltrate hospital networks by exploiting weak security protocols, outdated software, and unsecured devices.

5. Securing Hospital IT Infrastructure – The Role of Security Operation Centers (SOC)

- A Security Operation Center (SOC) acts as a Command & Control Center for monitoring hospital networks in real time.
- SOC frameworks can help hospitals detect and prevent attacks before they escalate.
- **Common cybersecurity loopholes in hospitals:**
  - **Weak hospital websites** – Many hospitals fail to implement strong security measures, making them easy targets for hackers.
  - **Unsecured routers & network devices** – Many hospitals use cheap, vulnerable routers that expose them to cyber threats.
  - **Lack of employee awareness** – Hospital staff unknowingly click malicious links, download unsafe apps, or fail to follow cybersecurity protocols.

6. Identifying & Eliminating Cybersecurity Vulnerabilities – CVE Analysis

- Common Vulnerabilities and Exposures (CVE) lists help hospitals identify security flaws in devices and software.
- Live demonstration: Mr. Irfan showed how a hospital could enter the brand name of their router, firewall, or any connected device into a CVE database to check if known vulnerabilities exist.
- Steps to secure hospital networks:
  - Run vulnerability scans on all hospital devices before purchasing or installing them.
  - Immediately replace or upgrade any devices flagged as high-risk.
  - Avoid using low-cost, unverified routers or network equipment, which can be easily compromised.

7. The Growing Risk of IoT (Internet of Things) & Unsecured Medical Devices

- Every connected medical device—from MRI scanners to patient monitoring systems—can be hacked if not properly secured.
- Live demonstration of SHODAN Tool – SHODAN helps identify vulnerable hospital devices, websites, and firewalls that could be easily exploited.
- Real-world example:
  - Many hospitals use low-security CCTVs for monitoring. If a hacker infiltrates the CCTV system, they can gain access to the hospital's entire network.
  - Similarly, biometric attendance systems are often connected to hospital networks but lack adequate protection, making them a weak point for hackers.

8. Dark Web & The Risks of Exposed Patient Data

- Stolen hospital data is sold on the dark web, often used for:
  - Medical fraud - e.g., fake insurance claims..
  - Identity theft - patient records are used for illegal activities.
  - Pharmaceutical scams - stolen prescriptions are resold illegally.
- Even "deleted" data can be retrieved using dark web tools, making proper data sanitization essential.
- Deep Web vs. Surface Web:
  - Only 8% of internet data is accessible through standard searches (Google, Bing, etc.).
  - 92% of sensitive data is stored in deeper, restricted layers of the web, meaning hospitals must take extra precautions to ensure their records are not accessible through unauthorized channels.

9. Strengthening Cybersecurity in Hospitals – Key Recommendations

- **Implement a Security Operation Center (SOC)** – Real-time network monitoring can prevent cyberattacks before they happen.
- **Invest in Secure Network Infrastructure** – Hospitals should avoid using unverified routers, insecure IoT devices, or weak encryption protocols.
- **Use CVE & SHODAN for Risk Assessment** – Regularly check hospital devices and network infrastructure for known vulnerabilities.
- **Train Hospital Staff on Cyber Hygiene** – Employees must be educated on phishing, malware, and safe browsing practices.
- **Encrypt All Patient Data** – Secure encryption ensures that even if data is stolen, it cannot be easily accessed.

Conclusion & Key Takeaways:

Mr. Irfan emphasized that cybersecurity is no longer optional for hospitals—it is essential for patient safety. He urged healthcare institutions to:

- Treat cybersecurity as a critical priority, not just an IT issue.
- Conduct regular security audits and identify weaknesses before hackers do.
- Establish a strong defense system through firewalls, encryption, and real-time monitoring.
- Invest in staff training to ensure that employees do not unknowingly expose hospital networks to cyber threats.

His session provided a critical wake-up call for hospitals, stressing that cyberattacks are inevitable, but preparedness can prevent catastrophic damage.

Mr. Irfan, Cybersecurity Analyst, CLFS, NALSAR University of Law

Session 5: Cybersecurity Challenges in Hospitals: Protecting Patient Data & Case Studies - Hospital Perspective

Speaker : Mr. Rejis Sen, VP Corporate Finance & M&A, Continental Hospitals

Mr. Rejis Sen provided a corporate hospital perspective on cybersecurity challenges in healthcare, focusing on the financial, operational, and reputational risks hospitals face due to data breaches and cyber threats. His session highlighted real-world incidents, key vulnerabilities in hospital IT infrastructure, and best practices for strengthening cybersecurity.

Key Discussion Points:

1. The Rising Threat of Cyber Attacks on Hospitals

- Hospitals are prime targets for cybercriminals due to the high value of medical data, which includes:
  - **Personally Identifiable Information (PII)** - e.g., names, addresses, Aadhaar numbers.
  - **Financial details** - e.g., insurance claims, billing records.
  - **Sensitive health data** - e.g., medical histories, prescriptions, and diagnostic reports.
- Cyberattacks can cause severe financial and reputational damage, leading to:
  - Loss of patient trust and lawsuits.
  - Disruptions in hospital operations - forcing hospitals to shift to manual processes.
  - Financial penalties for non-compliance with data protection regulations.

2. Major Cybersecurity Vulnerabilities in Hospitals

Mr. Sen outlined critical weak points in hospital IT infrastructure, including:

- **Outdated Software & Unpatched Systems** – Many hospitals fail to update their software regularly, leaving them vulnerable to known exploits.
- **Weak Network Security** – Poorly configured firewalls, unsecured routers, and lack of encryption increase the risk of cyberattacks.
- **Lack of Employee Awareness** – Human error is one of the biggest causes of data breaches, as employees often:
  - Click on phishing emails containing malware.
  - Use weak passwords or reuse login credentials across multiple systems.
  - Fail to recognize social engineering attacks that trick them into revealing sensitive information.
- **Third-Party Risks** – Hospitals often work with vendors, diagnostic labs, and IT service providers who may not have adequate security measures, making them potential weak links.

3. Financial & Operational Impact of Cyberattacks

Mr. Sen emphasized that cyberattacks can have long-term consequences, including:

- **Revenue Loss** – Cyber incidents lead to system downtime, disruption in billing, and patient service delays, resulting in financial losses.
- **Regulatory Fines & Legal Action** – Non-compliance with DPDP Act, GDPR, and HIPAA can result in hefty penalties.
- **Brand Damage & Loss of Patient Trust** – A single breach can permanently damage a hospital's reputation, affecting patient confidence and investor trust

5. Strategies for Strengthening Cybersecurity in Hospitals

Mr. Sen provided actionable recommendations for hospitals to improve cybersecurity and data protection:

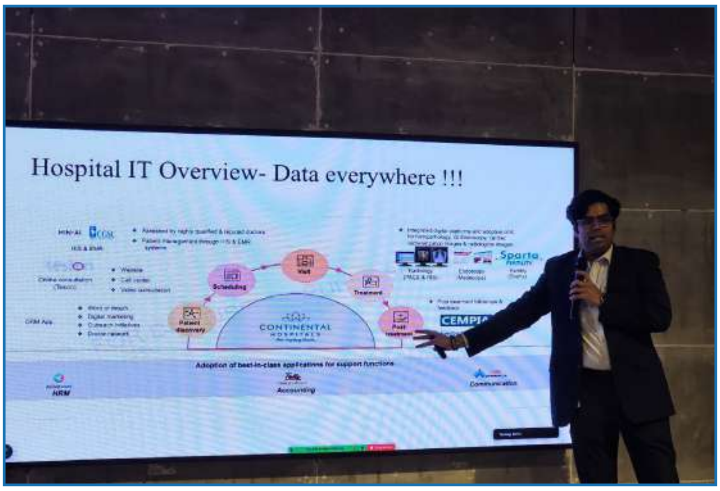
- **Implement Multi-Layered Security Measures:**
  - Strong firewalls & intrusion detection systems to monitor unauthorized access.
  - End-to-end encryption for protecting sensitive patient data.
  - Multi-factor authentication (MFA) to prevent unauthorized logins.
- **Regular Cybersecurity Audits & Penetration Testing:**
  - Conduct simulated cyberattacks to identify weak spots in hospital IT infrastructure.
  - Update & patch software regularly to prevent exploitation of known vulnerabilities.
- **Strengthen Vendor & Third-Party Security:**
  - Ensure all external service providers meet hospital security compliance standards.
  - Sign data-sharing agreements that define responsibilities and liabilities in case of a data breach.
- **Employee Training & Awareness:**
  - Conduct regular training sessions for hospital staff on phishing threats, password security, and safe data handling.
  - Implement strict access controls to ensure that only authorized personnel have access to sensitive patient data.

Conclusion & Key Takeaways:

Mr. Sen concluded by emphasizing that hospitals must invest in cybersecurity as a core business priority, not just a compliance requirement. He urged healthcare institutions to:

- Adopt a proactive cybersecurity strategy to prevent costly breaches.
- Implement stronger data governance and compliance measures to align with the DPDP Act, GDPR, and other global regulations.
- Integrate cybersecurity into hospital operations, ensuring IT security teams work closely with hospital administrators and medical staff.
- Recognize cybersecurity as an investment in patient safety, operational resilience, and long-term sustainability.

His session reinforced the urgent need for hospitals to prioritize cybersecurity, secure their digital infrastructure, and train their staff to mitigate emerging cyber risks in healthcare.



Mr. Rejis Sen, VP Corporate Finance & M&A, Continental Hospitals

Session 6: Cybersecurity Challenges in Hospitals: Protecting Patient Data & Case Studies - Start-up Perspective

Speaker : Mr. Vedant, Co-founder & CEO, Aarogya ID
Mr. Vedant discussed the vulnerabilities in hospital IT systems, citing outdated infrastructure, lack of cybersecurity awareness, and weak network security as major risks. He presented the AIIMS cyberattack case study, which highlighted the impact of ransomware attacks, data leaks, and operational disruptions.
To mitigate risks, he recommended:

- Multi-Factor Authentication (MFA) and strong access controls.
- Network segmentation to prevent single-point failures.
- Regular cybersecurity audits, software updates, and staff training.
- Backup and disaster recovery planning to restore data quickly after attacks.

He also emphasized the role of ABDM (Ayushman Bharat Digital Mission) in ensuring secure, tokenized, and consent-based healthcare data exchange, preventing unauthorized access and enhancing patient privacy.

Mr. Vedant, Co-founder & CEO, Aarogya ID

Session 7:Real-Time Practices and Success Stories - Industry Perspective

Speaker : Mr. Meeraj Kanaparthi, Senior Manager, Evernorth Health Services
Mr. Meeraj provided an industry perspective on cybersecurity threats in healthcare, citing ransomware, phishing, and third-party vulnerabilities as key concerns. He shared global case studies, including the AIIMS cyberattack and the Vastaamo breach, where poor encryption and weak access controls led to massive data leaks.
His recommendations included:

- Adopting a Zero-Trust Security Model and enforcing MFA.
- Proactive threat detection using AI-driven security solutions.
- Strengthening employee awareness and regular cybersecurity training.
- Ensuring compliance with data protection laws like DPDP Act, HIPAA, and GDPR

He emphasized that cybersecurity is critical for patient safety, and hospitals must integrate security measures into daily operations to prevent costly breaches.

Cybersecurity in hcare
Plan for the Unexpected
Develop contingency strategies to ad or data loss scenarios.
Control Access to Protected Health
Restrict PHI access to auth
Use Strong Passwords and Ch
Implement robust pas es.
Limit Network Access
Ensure that only aut etwork.
Control Physical Access
Secure physical areas housing ta to prevent unauthorized entry.

Mr. Meeraj Kanaparthi, Senior Manager, Evernorth Health Services

Session 8 : Interactive Session: Challenges, Solutions, and Future Directions

An interactive session provided an opportunity for participants to discuss challenges, solutions, and future directions in data protection and cybersecurity within healthcare.

Speakers:

- **Dr. Krishna Ravi Srinivas**, Adjunct Professor, NALSAR University of Law, led discussions on balancing innovation with data privacy regulations.
- **Dr. Sushmitha Sundar,** Head of Life Sciences, RICH, emphasized the importance of multi-stakeholder collaboration in securing digital health infrastructure.

The session concluded with an engaging Q&A segment, where participants raised critical questions on:

1. What is the applicability of the DPDP act in public health in India, especially in government hospitals and agencies?

The Act is applicable to all and the Act establishes a uniform framework for data protection across public and private healthcare entities. While government hospitals and public health agencies have certain operational flexibilities, they must comply with core data protection principles, ensuring secure, transparent, and responsible handling of patient information.

2. What measures do we need to take when dealing with the secondary data?

When dealing with secondary data, first understand its nature and purpose of use. Ensure compliance with data protection regulations, review data-sharing agreements, and apply security measures. Follow relevant guidelines and limit access to only necessary data while maintaining privacy and governance standards.

3. How long can we store Healthcare data?

The storage duration of healthcare data depends on the purpose and necessity. There is no strict constraint, but best practices suggest following industry standards and regulatory guidelines. If the data is no longer required, it should be securely deleted to prevent potential misuse or leaks. However, in cases where continued access is necessary (e.g., patient history, legal requirements), it can be retained for a longer duration, ensuring proper security measures are in place.

4. When we have to share patient reports to some other person like health camp healthcare, camp organizer or camp doctor, what kind of protection do we have to take?

When sharing patient reports, ensure recipient verification, secure transmission, necessary data only, proper authorization, and anonymization where possible to protect privacy and comply with regulations.

5. What are the biggest challenges healthcare providers face in implementing compliance while ensuring seamless, patient care?

Healthcare providers face challenges in balancing compliance with seamless patient care due to evolving regulations, interoperability issues, resource constraints, and cybersecurity threats. Hence, it is necessary to establish a Security Operations Center (SOC) and include data privacy and cyber security role and responsibility through administrative functions or consultants to ensure proactive compliance management, enhanced security, and uninterrupted patient care.

Closing Remarks and Networking

The workshop concluded with a closing note from Dr. Sushmitha Sundar, expressing gratitude to all, organizers, speakers, and participants. She emphasized the importance of continued awareness and collaboration to improve data security and compliance in healthcare.

Dr. Sushmitha Sundar - Head of Life Sciences - RICH

Insights & Recommendations

Strengthening Data Protection Laws in Healthcare

The Digital Personal Data Protection (DPDP) Act establishes a legal framework for safeguarding personal data, including sensitive health records, by mandating explicit patient consent for data collection and processing. It introduces principles such as purpose limitation, requiring that data be used strictly for its intended medical or research purpose, and data minimization, ensuring that only necessary information is retained. The Act also mandates secure storage and processing of health data and imposes penalties for non-compliance, reinforcing accountability among healthcare providers and data fiduciaries.

However, the Act lacks sector-specific provisions for healthcare, unlike the earlier proposed DISHA (Digital Information Security in Healthcare Act), which aimed to establish stringent security standards for medical data. Additionally, the DPDP Act does not specify a patient compensation model for individuals affected by data breaches, leaving a gap in accountability and legal recourse.

To strengthen data protection laws in healthcare, collaborative efforts among key stakeholders must be prioritized. Policymakers should work closely with healthcare institutions, legal experts, and technology providers to develop sector-specific guidelines that address the unique security and compliance challenges of medical data. Healthcare organizations must actively engage with cybersecurity firms and AI specialists to implement advanced security frameworks, ensuring patient data remains protected against emerging threats. Hospitals and research institutions should establish cross-industry collaborations to promote secure data-sharing models, standardized consent management systems, and real-time threat intelligence mechanisms. Additionally, fostering public-private partnerships can accelerate innovation in privacy-preserving technologies, regulatory compliance solutions, and ethical AI frameworks, ensuring a resilient, transparent, and patient-centric approach to digital healthcare security.

Implementing Robust Data Governance Frameworks

To establish a strong data governance framework, healthcare institutions must implement clear policies and structured oversight mechanisms to ensure data integrity, security, and compliance. A centralized data governance strategy should be developed to eliminate silos, standardize data management practices, and facilitate secure data sharing across departments. Organizations should define data ownership and accountability structures, ensuring that roles and responsibilities for data handling, processing, and protection are clearly assigned.

A comprehensive data classification system is essential for segmenting healthcare information into public, internal, confidential, and sensitive categories, enabling institutions to enforce appropriate security controls. To strengthen regulatory compliance, healthcare providers should align their governance frameworks with global data protection laws such as GDPR, HIPAA, and the DPDP Act. Implementing automated compliance audits and real-time monitoring systems will help institutions proactively identify and address security vulnerabilities. Additionally, regular data privacy assessments and risk evaluations should be conducted to ensure that governance policies remain up-to-date with evolving legal requirements.

Collaboration between healthcare administrators, IT teams, legal experts, and data protection officers is essential to build a scalable and adaptive governance framework. Training healthcare professionals on data governance best practices, patient data confidentiality, and cybersecurity protocols should be an ongoing initiative. By integrating robust governance structures, regulatory compliance mechanisms, and advanced security technologies, healthcare institutions can enhance patient trust, reduce legal risks, and create a more secure and efficient data management ecosystem.

Cybersecurity as a Critical Pillar of Patient Safety

As healthcare systems become increasingly digital, cybersecurity is no longer just an IT concern but a fundamental requirement for patient safety and operational stability. The rise in ransomware attacks, phishing schemes, and insider threats poses a significant risk to hospitals, where even a minor security breach can disrupt medical services, compromise sensitive patient data, and erode public trust. Outdated IT infrastructure, weak encryption, and limited cybersecurity awareness among healthcare professionals further amplify these risks. High-profile incidents, such as the AIIMS ransomware attack and data leaks from HealthifyMe and Kerala hospitals, highlight the severe consequences of inadequate security frameworks. Given the increasing value of healthcare data, hospitals must recognize cybersecurity as a critical pillar of digital transformation and take immediate action to strengthen their defenses.

To effectively combat cyber threats, hospitals must integrate cybersecurity into their core operations rather than treating it as an afterthought. Establishing Security Operation Centers (SOCs) will enable 24/7 threat monitoring and incident response, reducing the likelihood of breaches. Implementing Multi-Factor Authentication (MFA) and role-based access control (RBAC) can significantly minimize unauthorized access to sensitive patient records. Routine penetration testing and vulnerability assessments will help identify and address security gaps before they can be exploited. Leveraging AI-driven threat detection systems can further enhance hospitals' ability to proactively identify and neutralize cyber risks.

Beyond technological defenses, fostering a culture of cybersecurity awareness is equally crucial. Hospitals should conduct regular training programs for healthcare professionals to educate them on phishing detection, secure data handling, and cyber hygiene best practices. Establishing clear incident response protocols ensures that, in the event of a cyberattack, damage is contained swiftly with minimal disruption to patient care. By prioritizing proactive security strategies, healthcare institutions can build a resilient defense against cyber threats, ensuring the protection of patient data and the continuity of critical healthcare services.

सत्यमेव जयते

Office of the Principal Scientific Adviser
to the Government of India

RICH
Research and Innovation
Circle of Hyderabad

Research and Innovation Circle of Hyderabad

RICH, Cabin No. 16, T-Hub Foundation,
Plot No 1/C, Sy No 83/1, Raidurgam Panmaktha,
Hyderabad Knowledge City,
Hyderabad, Telangana – 500081
Email: cmanager-rich@telangana.gov.in