the-tech-trend.com

Cybersecurity Challenges, Best Practices, and Future Work in Healthcare

Arash Habibi Lashkari

27–34 minutes

Cybersecurity Concerns in Digital Healthcare

As healthcare professionals, IT professionals, and decision-makers in healthcare organizations, your role in exploring and addressing the potential security and privacy concerns in healthcare systems is crucial and highly valued. (Jawad, 2024). Figure 10.1 shows the key potential cybersecurity concerns in digital healthcare systems. These common potential security concerns and the best practices that are used to ensure security and privacy in the healthcare industry are discussed as follows:

- **Data breaches and unauthorized access**: Data breaches can occur due to various factors, including vulnerabilities in software systems, weak authentication mechanisms, or inadequate security protocols. To address these concerns, a healthcare organization can implement robust security measures such as secure storage methods and strong access controls to protect patient data at rest and in transit.

- **Cybersecurity attacks:** Potential cyberattacks such as ransomware attacks, malware infections, phishing attempts, and DDoS attacks can disrupt healthcare services, compromise the confidentiality and integrity of patient data, and even impact patient safety. To protect from these attacks, a healthcare organization can adopt multi-layered approaches such as firewalls, intrusion detection systems (IDS), and anti-virus software. Regular vulnerability assessments and penetration testing can help identify and address potential vulnerabilities before exploiting them. The most common way to protect patient data from ransomware attacks is to keep data backup up-to-date and change all your credentials as soon as possible. DDoS attacks can be protected by using network and application monitoring tools and identifying traffic trends and patterns. Keeping your device and software updated, using a non-administrator account, and not opening emails and other attachments from unknown or untrusted senders can help reduce malware attacks. Educating your employees and conducting training sessions with mock phishing scenarios and simulations could help prevent Phishing attacks.
- **Insider threats:** An insider threat is a malicious threat to a healthcare organization from current employees, former employees, contractors, business associates, and others with access to patient data and IT systems. To address insider threats, a healthcare organization should implement role-based access controls, ensuring that employees only have access to the data necessary for their job responsibilities. Monitoring suspicious activities enables timely intervention in case of unauthorized access or data misuse.
- **Medical and IoT device integration**: Integrating medical devices

and Internet of Things (IoT) devices in healthcare introduces additional cybersecurity risks. For example, pacemakers, insulin pumps, or connected IoT wearables to healthcare networks can become a potential target for attackers. Exploitation of security vulnerabilities in these devices can lead to unauthorized access, tampering, or disruption of healthcare services. To mitigate these vulnerabilities, healthcare organizations can adopt risk assessments, regular software updates and patches, and implement robust authentication mechanisms to access the devices.

- **Big data analytics**: Using big data analytics in healthcare can raise privacy issues. It reveals detailed information on an individual patient's health conditions, behaviors, and lifestyle choices, which increases the risk of potential re-identification and the misuse of personal information. To address these concerns, privacy-enhancing technologies such as differential privacy can be employed to protect patient privacy while enabling valuable data analysis. Standards and compliance with privacy regulations ensure patient privacy.

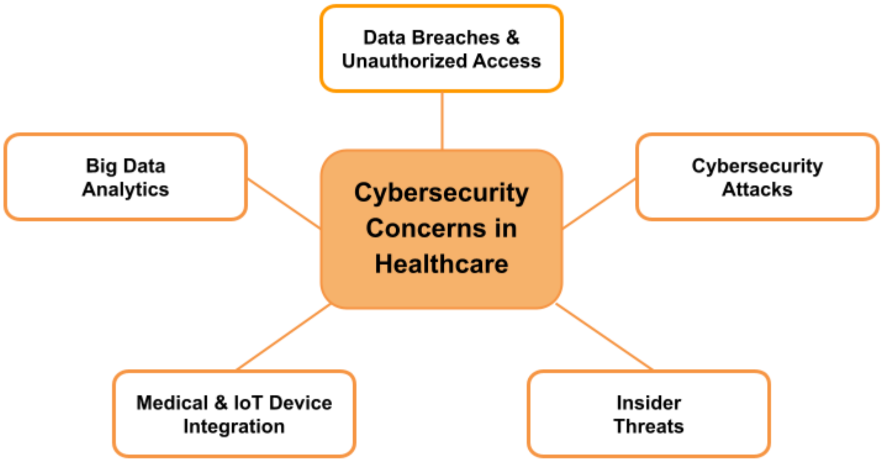
Data Breaches & Unauthorized Access
Big Data Analytics
Cybersecurity Concerns in Healthcare
Cybersecurity Attacks
Medical & IoT Device Integration
Insider Threats

Figure 10.1: Key cybersecurity concern in healthcare

Mitigation methods for security and privacy concerns in healthcare

Security and privacy are critical considerations in a modern digital healthcare system. Figure 10.2 shows the essential mitigation methods for protecting healthcare data from future cyberattacks. These methods are considered the best practices and can be used to ensure security and privacy in the healthcare industry. These methods are described as follows:

- **Two-factor authentication and biometric verification:** Robust authentication and access control mechanisms help mitigate security and privacy concerns in healthcare systems. Robust authentication methods such as two-factor or biometric verification can help ensure that only authorized individuals can access patient data. Role-based access controls should be implemented to limit access privileges based on job responsibilities and the principle of least privilege.
- **Encryption and data protection:** The encryption methods ensure that data remain confidential. Robust encryption algorithms can be used to encrypt data both at rest and during transmission. Additionally, healthcare organizations can employ secure storage methods and backups to prevent data loss or unauthorized modifications.
- **Continuous security monitoring:** Healthcare system operational and network traffic activities can be monitored by implementing advanced intrusion detection systems (IDS) and intrusion prevention systems (IPS) or security information and event

management solutions. These security monitoring systems can help identify and respond to threats in real time.

- **Incident response planning and handling:** The impact of cybersecurity attacks can be minimized by preparing a well-defined incident response plan that includes containment, eradication, and recovery procedures.
- **Cybersecurity literacy and awareness training:** Continuous training and awareness programs are very important for healthcare professionals and staff to understand potential cyber threats and best practices. The training topics can include password hygiene, identifying phishing attempts, secure data handling practices, etc. Ensuring employee awareness of their roles, responsibilities, and data security and privacy obligations can improve cybersecurity.
- **Strong data security measures and risk assessment:** Employ state-of-the-art encryption algorithms, firewalls, and intrusion detection systems to protect patient data from unauthorized access or breaches. Healthcare organizations can leverage the NIST Cybersecurity Framework, which guides them in managing cybersecurity risks and helps protect patients and other sensitive information. It allows an organization to determine its cybersecurity goals, assess its current cybersecurity practices, or lack thereof, and help identify gaps for remediation (NIST, The NIST Cybersecurity Framework (CSF) 2.0, 2024). A risk-based assessment scans the healthcare system to identify, investigate, and prioritize the most critical assets and vulnerabilities. The selection of the proper cybersecurity risk assessment and management tools is crucial to the healthcare industry for identifying, prioritizing, and mitigating cyber risks. Organizations should carefully evaluate their requirements, budget, and

regulatory compliance and select the security and risk assessment tools that meet their security requirements. This evaluation can be carried out in consultation with cybersecurity experts. Vulnerability scanning tools are used to find security loopholes and risks in the networks and systems. Nessus (Nessus, 2024) and OpenVAS (OpenVAS, 2024) are two standard vulnerability scanning tools. Regular security audits and risk assessments can help identify vulnerabilities and update systems with the latest security practices.

- **Compliance with privacy regulations and standards:** Healthcare organizations should ensure compliance with relevant data privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States (HIPPA, 2023) or the General Data Protection Regulation (GDPR) in the European Union (GDRP, 2024). These frameworks outline guidelines for handling patient data, ensuring privacy, and maintaining data integrity. Compliance with these regulations and standards ensures that commitment to privacy and data protection of patients’ personal and healthcare information is handled responsibly and lawfully.

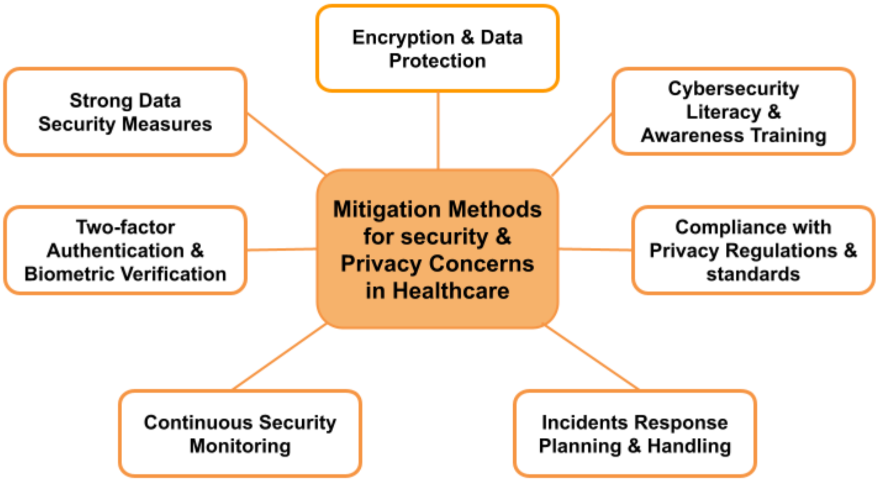
Encryption & Data Protection
Strong Data Security Measures
Cybersecurity Literacy & Awareness Training
Two-factor Authentication & Biometric Verification
Mitigation Methods for security & Privacy Concerns in Healthcare
Compliance with Privacy Regulations & standards
Continuous Security Monitoring
Incidents Response Planning & Handling

Figure 10.2: Mitigation methods for security and privacy concerns in healthcare

Five Key Cyberattacks and Best Practices in Healthcare

Ransomware, DDoS, insider threats, malware, and phishing attacks are the five vital potential cyberattacks in digital healthcare systems (Salama, Altrjman, & Al-Turjman, 2024). Figure 10.3 shows the five critical cyberattacks in the healthcare industry. Similarly, Table 10.1 summarizes the cybersecurity best practices for protecting from these five cyberattacks in healthcare. The descriptions of these five cyberattacks with their best practices are as follows:

- **Ransomware attacks:** A ransomware attack is a type of malware in which hackers encrypt your critical data so that you cannot access it until you pay the demanded ransom. The most common way to protect your data from ransomware attacks is to keep a backup and change all your credentials as soon as possible.
- **DDoS attack**: A DDoS attack is another potential cyberattack in healthcare systems. Cybercriminals flood a network with malicious, harmful traffic that prevents normal operation and communication. There are several ways to prevent your devices from DDoS attacks. For example, secure your router by changing the default password, use network and application monitoring tools to identify traffic trends and patterns, etc.

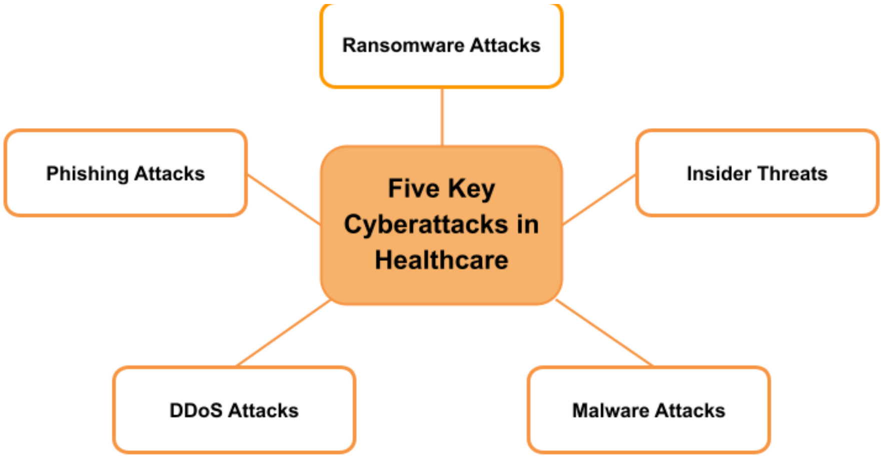

Figure 10.3: Five key cyberattacks in healthcare.

- **Insider threat:** An insider threat is a malicious threat to an organization from current employees, former employees, contractors, business associates, and others with access to critical data and IT systems. Policies, procedures, and technologies that help prevent privilege misuse can manage insider threats. Tools such as continuous risk assessment, security incident management, automatic monitoring, etc., can help mitigate internal threats.
- **Malware attacks**: A malware attack is a typical cyberattack where malicious software executes unauthorized actions on your system. The malicious software performs different attacks, such as ransomware, spyware, trojans, worms, viruses, etc. Keeping your device and software updated, using a non-administrator account as much as possible, not opening emails and other attachments from unknown or untrusted senders, etc., can help to reduce the malware attack.
- **Phishing attacks**: Phishing is a most common type of social engineering attack where an attacker sends a fraudulent message using email, social media, instant messaging, SMS, or phone calls

to obtain sensitive personal information from the victims. Attackers can use different methods of phishing. For example, phishing via emails, vishing, and smishing. Phishing via email is the most common phishing attack method, and attackers use spam emails, malicious websites, or malware attachments. Two-factor authentication, VPN services, and regular cybersecurity awareness training can help protect your system or data from phishing attacks.

Table 10.1: Cybersecurity best practices for protecting from the potential common cyberattacks in healthcare.

Potential cyberattacks	Key best practices
Ransomware attacks	Keep data backup up to date. Change user credentials as soon as possible. Keep your device's software updated.
DDoS attacks	Use network and application monitoring tools to identify traffic trends and patterns.
Insider threats	Use continuous risk assessment and automatic incident monitoring tools. Define proper security policies and procedures.
Malware attacks	Keep your device and software updated. Using a non-administrator account as possible. Do not open emails and other attachments from unknown or untrusted sender.

Phishing attacks	Educate your employees about the phishing attacks with training sessions. Conduct mock/simulated phishing scenarios.

Challenges of Personal Cybersecurity in Healthcare

Healthcare systems face challenges in safeguarding personal data and privacy from cyber threats and ensuring the system's integrity. Here are some of the main challenges:

- Preventing identity theft and fraud by protecting personal data.
- Ensuring the accessibility of EHRs with adequate security measures to prevent data breaches.
- Assuring the security and privacy of personal data when using online healthcare platforms.
- Increasing individual awareness and training on cybersecurity threats, such as phishing emails and other cybercrime tactics.
- Providing secure networked medical devices to prevent cyber attackers from accessing and manipulating personal data.
- Maintaining a secure environment to prevent hackers from targeting unpatched vulnerabilities in outdated legacy systems within healthcare organizations.

While these are some of the most common personal cybersecurity challenges, other cybersecurity challenges are specific to patients or healthcare professionals, such as doctors and staff, as outlined below:

Challenges of Patient Cybersecurity in Healthcare

- Maintaining patient trust in their privacy and the competence of the healthcare system.
- Protecting patients' sensitive medical records against ransomware, malware, DDoS attacks, and data breaches to prevent identity theft and fraud.
- Protecting patient data from unauthorized access by encrypting it.
- Protecting patient data security and privacy when using remote healthcare services.

Averting adverse effects on patients, such as delayed treatments, medication errors, and inaccuracies in diagnosis and treatment caused by cyberattacks on health and well-being.

Also read: Cybersecurity Governance and Ethics in Healthcare

Challenges of Doctors' Cybersecurity in Healthcare

- Balancing allocating resources for cybersecurity while prioritizing personal healthcare needs within a limited budget.
- Keeping a balance between clinical focus and cybersecurity to mitigate doctors' vulnerabilities.
- Implementing cybersecurity measures to safeguard their privacy and professional reputation from cybersecurity breaches.
- Targeting their information prevents cybercriminals from causing significant financial losses and identity theft.
- Assuring patient privacy and protecting sensitive information.
- Integrating cybersecurity practices into healthcare delivery, preventing cyberattacks that delay treatment and misdiagnose patients, and protecting patients from data corruption and

ransomware.

Challenges of Staff Cybersecurity in Healthcare

- Preventing data breaches, cybersecurity threats, phishing emails, and other cybercrime tactics by continuous training and awareness.
- Maintaining vigilance to recognize cyber threats and prevent security errors, especially during heavy workloads.
- Keeping up with evolving threats through continuous education.

Challenges of Software Security in Healthcare

The security of healthcare software faces numerous challenges that threaten the confidentiality of patient data, the integrity of the system, and the safety of patients. Some of these challenges include:

- Managing credentials effectively to avoid issues such as poor default usernames, weak passwords, and hard-coded credentials.
- Addressing buffer overflow vulnerabilities, the most common software vulnerabilities, by improving software design and testing practices to prevent program crashes and protect patient health and sensitive medical data.
- Enhancing authentication security and reducing the risk of unauthorized access by eliminating hard-coded credentials and implementing an “initial login” mode requiring solid and distinct passwords
- Protecting patient data from interception and unauthorized access by implementing robust encryption.

- Preventing legacy systems and outdated software from becoming easy targets for cyberattacks due to limited vendor support by updating them.
- Mitigating insider threats by enhancing access protocols, retraining employees, imposing sanctions, and taking corrective actions to prevent unauthorized access and disclosure of sensitive information.
- Managing third-party involvement in healthcare software to reduce the risk of security breaches by implementing robust cybersecurity measures and addressing challenges posed by technologies like cloud computing.
- Ensuring patient safety and system integrity by securing communication channels and network schema and following secure software practices.
- Protecting healthcare software against cyberattacks by continuously monitoring security.

Challenges of Infra-Security in Healthcare

Addressing infra-security challenges in healthcare is essential for protecting patient data, ensuring seamless healthcare delivery, preventing cyber threats, and, thus, maintaining the integrity and confidentiality of sensitive information. Some of these challenges are:

- Ensuring the confidentiality, integrity, availability, ownership, and privacy of healthcare information to protect sensitive data.
- Implementing effective control and audit mechanisms to monitor and secure healthcare data.

- Protecting healthcare infrastructures and networks from unauthorized access, vulnerabilities, and cyber threats.
- Preventing identity theft, tax fraudulence, medical fraud, bank fraud, and insurance fraud.
- Protecting the privacy and reputation of high-profile patients from defamation and data breaches.
- Extending and securing health applications on tablets, laptops, and smartphones.
- Preventing data breaches, data loss, and account hijacking.
- Providing strong authentication, authorization, and access control.
- Ensuring secure data access, safe data transmission, and deleting data when no longer needed.
- Securing interfaces and APIs against vulnerabilities and misuse.
- Protecting against hackers, as well as malicious insiders.

Challenges of Apps Security in Healthcare

- Managing large volumes of medical data from a variety of sources by using advanced machine learning algorithms and data processing techniques.
- Avoiding compatibility and security issues by developing standardized communication protocols among devices and systems.
- Updating outdated infrastructure and integrating modern healthcare apps.
- Ensuring data unification by making diverse healthcare devices compatible and enabling seamless data exchange for effective

data use.

- Ensuring healthcare apps comply with varying privacy and security regulations across countries and regions.
- Investing in secure healthcare apps and infrastructure requires significant investment with long-term benefits, which justifies the cost factor.
- Building trust with patients, healthcare providers, and the public regarding data usage through transparent communication and strategies.
- Implementing robust authentication and access control measures to protect sensitive data.
- Preventing cloud resource abuse and ensuring proper management and security of cloud-based healthcare apps.
- Securing mobile devices that access healthcare apps against threats such as malware, loss, and unauthorized access.
- Training users to recognize and avoid cyber-attacks.
- Implementing continuous monitoring of healthcare apps and having an effective incident response plan to address security breaches quickly.

Addressing these challenges requires a comprehensive approach to healthcare software security, including implementing robust authentication mechanisms, encrypting sensitive data, regularly updating software and systems, conducting security audits and assessments, and fostering a culture of security awareness and compliance throughout the organization. By proactively addressing these challenges, healthcare organizations can mitigate the risk of healthcare software security vulnerabilities.

Also read: Detection and Prevention of Cyber-attacks in Healthcare

Cybersecurity Best Practices for Healthcare Professionals and IT Systems Administrators

Healthcare professionals and IT systems administrators play crucial roles in safeguarding modern digital healthcare systems. As these two users have different roles and responsibilities, they can implement different cybersecurity best practices so that the deployed best practices can significantly enhance the security posture of their healthcare organizations, protect sensitive patient data, and maintain the trust of their patients. Based on their roles, ten common best practice activities with their outcomes are discussed.

Healthcare Professionals

Healthcare professionals such as doctors, nurses, and other clinical staff play a significant role in maintaining the security and privacy of patient data. Applying cybersecurity best practices significantly enhances the security posture of healthcare systems. The common 10 security best practices for healthcare professionals are summarized in Table 10.2.

Table 10.2: Cybersecurity Best Practices for Healthcare Professionals

Activities	Outcomes
Use Strong Password and Multi-Factor	Reduce the risk of unauthorized access.

Authentication (MFA)	Protect sensitive data.
Ensure patient data encryption both at rest and in transit	Protect patients from unauthorized access to healthcare data at rest and in transit.
Use VPN, Firewall, and IDS	Monitor network traffic and protect the internal network from unauthorized access and malicious activity.
Keep regular software updates.	Enhance features, functionalities, and performance. Fixed bugs and security holes. Protect from malware (e.g., ransomware) and sophisticated attacks.
Secure physical access to devices with strong passwords	Enhance data protection. Protect patient data.
Install and maintain advanced antivirus and anti-malware software	Detect a wide variety of malware, including viruses, Trojans, ransomware, spyware, etc., and help mitigate the risk of malware infections. Reduce the risk of data breaches.
Report incident	Minimize the impact of the incident. Prevent future attacks.
Ensure Regulatory Compliances	Ensure security measures comply with regulatory compliances (e.g., HIPAA, GDPR, etc.) requirements and other relevant regulations.

Participate in cybersecurity awareness training.	Stay informed about the latest cyber threats and state-of-the-art best practices.
Educate patients	Educate patients on how to protect their healthcare information when accessing online healthcare services and data.

IT and Systems Administrators

Information Technology (IT) and System Administrators are specialized professionals responsible for managing and maintaining the information technology and network infrastructure that supports healthcare services. IT and system administrators can significantly enhance the security posture of healthcare organizations, protect sensitive patient data, and ensure compliance with regulatory requirements by applying these security best practices. The common 10 security best practices for IT and system administrators in healthcare systems are summarized in Table 10.3.

Table 10.3: Cybersecurity Best Practices for IT and Systems Administrators.

Activities	Outcomes
Risk and Vulnerability Analysis	Identify, prioritize, and mitigate cybersecurity risks and vulnerabilities.
Access Control and Identity Management	Prevent unauthorized access to systems and data.

Vulnerability and Patch Management	Prioritize patching based on the severity of vulnerabilities and their impact on healthcare systems and services. Ensure installed applications software, operating systems, and underlying firmware are regularly updated with the latest security patches.
Implements Firewalls, IDS, and IPS	Monitor network traffic and protect the internal network from unauthorized access and malicious activity.
Deploy Endpoint Detection and Response (EDR) Tools	Detect and prevent malware infections. Provide remediation suggestions to restore affected systems. Manage and secure all endpoint devices, including desktop computers, laptops, mobile devices, servers, and other medical devices.
Prepare Incident Response Plan	Outlines procedures (plan) for detecting, responding, and recovering from potential future cyberattacks.
Implement Advanced Data Encryption and Data Loss Prevention Solutions	Protect from unauthorized access to patients and other sensitive healthcare data at use, rest, and transit.

	Secure data being used by health information system applications or endpoint systems. Protect data stored at network locations/sites (on-premises or cloud). Ensure the safe transmission of patient-sensitive data while it moves across the network.
Use Continuous Monitoring Tools	Detect and respond to cyberattacks in real-time. Protect the healthcare systems from emerging cyber threats and vulnerabilities.
Regulatory compliance	Ensure security measures comply with regulatory compliances (e.g., HIPAA, GDPR, etc.) requirements and other relevant regulations.
Training and Awareness	Educate all healthcare professionals and staff on cybersecurity threats, best practices, policies, and procedures.

Also read: Defining Cybersecurity in Healthcare

Cybersecurity Future Work in Healthcare

Cybersecurity concerns in the healthcare sector are growing as the value of sensitive healthcare and digitalized personal health records become more widely available (Salama, Altrjman, & and Al-Turjman, 2024). The future of cybersecurity in healthcare necessitates a forward-looking approach to address emerging cyber threats and ensure the protection of sensitive patient data and healthcare systems. Here are some areas for cybersecurity future work in healthcare:

- **Privacy-enhancing technologies:** The development of privacy-enhancing techniques, including differential privacy, secure multi-party computation, and homomorphic encryption, is imperative for enabling privacy protection while collecting and analyzing data collaboratively. (Liu, Zhang, Yang, & Meng, 2024).
- **Federated Learning (FL) and Differential Privacy (DP):** FL and DP are two innovative technologies that offer a powerful approach to enhancing the privacy and security of healthcare data. These methods allow for patient-sensitive data in research and analytics without compromising individual privacy. Federated learning is a decentralized approach to machine learning where the patient's data remains on local devices and only model updates. This method enhances privacy and security by keeping sensitive data within the local environment. It significantly helps preserve patients' private data from being exposed to attackers. DP is a mathematical framework that provides a quantifiable privacy protection measure when medical data analysis is done. It introduces noise into the data or the query results, ensuring that the inclusion or exclusion of a single data point does not significantly affect the outcome, thus protecting individual data points. In recent years, there has been a surge in the development of novel algorithms for differential privacy for healthcare data analysis (Brisimi, et al., 2018) (Wei, et al., 2020).
- **Securing Medical Things (IoMT) devices**: IoMT is a significant application of the IoT that benefits human welfare; it also presents

security and privacy risks in collecting and processing healthcare data. Quantum blockchain can provide a higher level of security for handling medical data involving the Internet of Medical Things (IoMT) (Qu, and Meng, and Liu, and Muhammad, & and Tiwari, 2024). Quantum blockchain is to combine quantum technology and blockchain. Blockchains are publicly distributed ledgers that record information and enable tamper-proof data storage by continuously adding new blocks.

- **Postquantum cryptography:** Cryptographic algorithms (e.g., lattice-based, hash-based, code-based, and multivariate polynomial cryptosystems) are resistant to quantum attacks. Integrating post-quantum cryptography, searchable encryption, and blockchain technology can be used for security and privacy preservation in healthcare (Xu et al., 2022). Combining post-quantum public-key searchable encryption and blockchain methods protects against current and future cyber threats and facilitates efficient and compliant data sharing and collaboration among healthcare stakeholders.

Summary

This blog delves into cybersecurity challenges, state-of-the-art best practices, and future healthcare data privacy and security work. It presents security and privacy concerns in healthcare with best practices and cybersecurity mitigation methods for security and privacy concerns in healthcare, identifying the potential five common cyberattacks and best practices used to protect healthcare data. It also presents cybersecurity challenges for patients, doctors, infrastructure, software, apps, etc. It lists the cybersecurity best practices for healthcare professionals and IT systems administrators. Finally, we discussed some potential future research directions in healthcare data privacy.