Implementing HIPAA Compliant Cybersecurity for Healthcare SMEs using BDSLCCI Framework

Shekhar PAWAR
Doctor of Business
Administrator (DBA)
Swiss School of Business
Management
Switzerland
Jaganathan T
HIPAA Auditor and Trainer
Bachelor of Engineering
Annamalai University
India.

Abstract

Cyberattacks on the healthcare industry have profound and far-reaching consequences, affecting patient safety, financial stability, service availability and trust in healthcare systems. Several countries have different data protection acts that are already playing an essential role in maintaining privacy, security, and trust in the digital age. A US federal law known as the Health Insurance Portability and Accountability Act (HIPAA) attempts to safeguard the confidentiality, integrity, and security of Protected Health Information (PHI and ePHI), which comprises sensitive patient data such as financial information, Social Security numbers, and medical records. In spite of this, numerous healthcare organizations around the world are being targeted by cyberattacks. Small and medium-sized businesses (SMEs) in particular face difficulty putting cybersecurity measures into place. To address those concerns and the growing need for cybersecurity protections, the Business Domain Specific Least Cybersecurity Controls Implementation (BDSLCCI) is providing a new framework that considers the Defense in Depth (DiD) and Confidentiality, Integrity, and Availability (CIA Triad) concepts. The author will explain how the BDSLCCI framework can be mapped to the cybersecurity needs and compliance requirements of hospitals and other SMEs in the healthcare industry.

Keywords: *Healthcare; SME; HIPAA; Cybersecurity; BDSLCCI; Data Protection Act*

1. INTRODUCTION

The healthcare industry is a dynamic sector involving hospitals, clinics, pharmaceuticals and biotechnology, medical devices, health insurance, public health organizations, and digital health and telemedicine. It focuses on preventing, diagnosing, treating, and managing illnesses and injuries, promoting healthy behaviors, and addressing community health needs through digital health and telemedicine [1, 2].

Cybercriminals are constantly targeting the healthcare sector. The DeepBlueMagic ransomware attack that Hillel Yaffe experienced on October 13, 2021, resulted in the encryption and locking of all hospital computer systems at all levels. The attack bypassed security tools by employing cutting-edge encryption techniques. To disable computers, the attackers employed legitimate programs like Microsoft BitLocker. The National Cyber Council and the National Ministry of Health were informed of the attack. In order to stop additional harm from affecting patient data, communication systems, and medical services, the Hillel Yaffe Medical Center (HYMC) promptly locked internet access. An incident at the hospital resulted in a loss of data that affected patient information, electronic medical records, inpatient lists, outpatient appointments, laboratory services, and imaging availability. A recovery process started on the first day after the online staff communication system was shut down. After eight weeks, email and intranet communication were reestablished, enabling the hospital administration to progressively resume regular operations and assess the resulting changes. Healthcare institutions have been targeted multiple times, potentially leading to financial disruptions and loss of life due to delayed or preventive critical care. Several papers discussed methods to prevent, recover, and analyze such attacks, highlighting their potential impact on healthcare systems [3]. Between 2019 and 2023, notifiable healthcare data breaches in Australia indicate 20% of healthcare information leakage incidents [6].

Globally, 1,463 cyberattacks occurred every week in 2022, jeopardizing medical service resources and access. Hospitals are forced to pay a ransom or face a 24-day outage, which costs $10 million on an average. A simultaneous cyberattack at two or more nearby hospitals would be a nightmare scenario since it might affect patients with urgent diagnoses' access to care. Cybercriminals offered patients $50 to have their private health information taken down from the dark web during a cyberattack on Seattle's Fred Hutchinson Cancer Center in November 2023. Threats of swatting were given to patients who refused. Cybercriminals attacked Liberty Hospital (LH) in Missouri, USA on December 19, 2023, and sent a ransom note to the hospital management via fax. The emergency department was closed to trauma, code stroke, code STEMIs, direct admissions, and incoming transfers when LH went into downtime. Patients in need of transfer services received midwestern hospitality from nearby hospitals. By the end of the first day of the attack, more than half of the patients had been moved to nearby hospitals or released from LH [8].

In November 2022, a major ransomware attack occurred at the All-India Institute of Medical Sciences (AIIMS) in New Delhi, one of India's top medical schools. For almost two weeks, the attack interfered with the hospital's digital operations, impacting its vital systems, including the database that held patient information. Thousands of patients and medical staff were unable to access vital services and records as a result of the attack, underscoring the increasing susceptibility of Indian healthcare institutions to cyberattacks. To decrypt the data, the attackers demanded a ransom in cryptocurrency worth about ₹200 crore. Concerns regarding cybersecurity in Indian healthcare were raised by the incident, which attracted media attention. Investigating the attack and attempting to restore the systems were done with the involvement of the Delhi Police cybercrime division and the Indian Computer Emergency Response Team (CERT-In). A ransomware attack on the eHospital platform at AIIMS, that treats over 10,000 patients every day, caused serious disruptions in patient care. Treatment delays and a greater workload for medical staff resulted from the disruptions to the outpatient department, inpatient management system, blood bank services, and appointment systems. Delays in patient care and a detrimental effect on lives resulted from the operational inefficiencies created by the disruptions. Response times were slower, and care plans were less successful when patient data was managed manually. Despite these shortcomings, post-attack actions were taken to improve cybersecurity at AIIMS and other hospitals [9].

Use of Internet of Things (IoT) devices in healthcare has completely changed patient care by enhancing monitoring, diagnosis, and treatment. But serious cybersecurity issues have emerged as a result. A multifaceted strategy is required to address these, which includes strengthening device security, putting strong security measures for networks, strict compliance to the regulations, and encouraging a security-conscious culture among medical staff. Strong authentication procedures, frequent firmware updates, network segmentation, intrusion detection systems, and encryption are important tactics. Complying to security and data protection regulations such as HIPAA and GDPR is essential for maintaining legal compliance and strengthening healthcare organizations' security posture. Wearable, implanted, smart medical, ambient, research and development, and healthcare operation systems are some of the subcategories of healthcare IoT devices. Smart medical equipment includes diagnostic, therapeutic, and patient care devices; wearable devices which track physiological parameters; and implantable devices which track specific medical conditions. Recent research reports of 2024 on cyberattacks on IoT devices in the healthcare industry show that DDoS attacks against healthcare systems have risen by 35% from the year before, with over 50% of these attacks caused by insecure IoT devices. The necessity for improved network defenses is highlighted by the fact that nearly 47% of healthcare organizations had a DDoS attack within the previous two years. IoT-enabled medical devices are increasingly being the target of man-in-the-middle (MITM) attacks, which have the potential to compromise real-time patient monitoring systems and result in serious consequences. Incidents of healthcare IoT malware have also surged, rising by 60% in 2023 compared to the previous year. Medical device vulnerabilities are exploited by botnets such as Mirai, underscoring the necessity of proactive threat detection systems [10].

According to the most recent research study, ransomware attacks have a major impact on acute patient care, Early Detection workflow, and the personal wellbeing of healthcare professionals in hospitals. There is frequently little preparation for such events, and there are numerous difficulties during the attack's acute and recovery phases [11].

All these evident and rising cyber threats on the healthcare industry need to be addressed for the relatively small and medium sized organizations or hospitals as well. All HIPAA regulatory requirements are to be complied with by all the entities in the USA handling PHI and ePHI irrespective of their size, be it a small physician clinic or a laboratory.

2. Cyber Threats In Healthcare Industry

According to recent studies, stakeholders who use medical implant devices are currently confronted with an expanded threat and vulnerability landscape. Healthcare is undergoing a revolution including medical implants. In addition to providing remote monitoring, few of these devices can deliver therapy when necessary. By permitting communication between Medical Internet of Things (mIoT) sensors and devices via the Internet, healthcare providers are exposing their patients to risk for vulnerabilities especially of the IoT devices. Because medical implants rely on external communication to transmit and receive data, these devices are vulnerable to cyberattacks if cybersecurity best practices are not followed. Vulnerabilities in privacy and security have thus emerged as significant issues for mIoT devices. Researchers have reached a critical point where fixing security flaws is necessary to ensure that mIoT devices continue to be used, despite their many advantages [7].

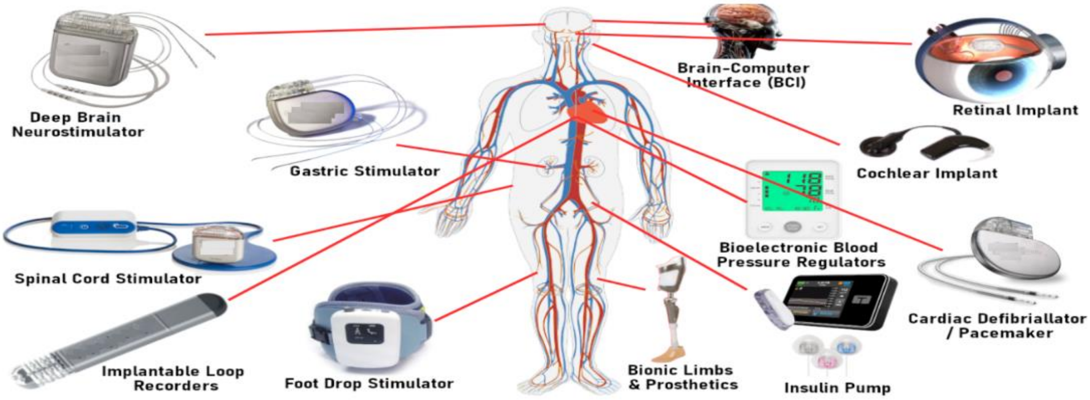
Deep Brain Neurostimulator
Brain-Computer Interface (BCI)
Retinal Implant
Gastric Stimulator
Cochlear Implant
Bioelectronic Blood Pressure Regulators
Spinal Cord Stimulator
Cardiac Defibriallator / Pacemaker
Implantable Loop Recorders
Foot Drop Stimulator
Bionic Limbs & Prosthetics
Insulin Pump

Figure 1: Medical Digital Implants for Human Body

Figure 1 shows diagrammatic examples of a few popular medical digital implants for human body. Refer to table 1 showing these medical digital implants for the human body and possible cyber threats with recommended solutions [14, 15, 16, 17].

TABLE 1. OVERVIEW OF HIPPA

Medical Digital Implant	Possible Cyber Threats	Recommended Solutions
Deep Brain Stimulator (DBS)	• Unauthorized remote manipulation • Data privacy leaks • Wireless jamming of signals	• Strong encryption for communication • Multi-factor authentication • Regular firmware updates
Brain-Computer Interface (BCI)	• Neural data interception AI manipulation • Malware affecting cognitive functions	• End-to-end encrypted neural data • Secure AI integration with verifiable algorithms • Zero-trust architecture for access control
Spinal Cord Stimulator	• Remote hacking altering pain modulation • Ransomware targeting implant settings • Unauthorized data extraction	• Robust encryption • Backup secure configurations • Hospital network segmentation to prevent lateral attacks
Smart Pacemakers and Defibrillators	• Life-threatening unauthorized adjustments • Wireless protocol vulnerabilities • Denial-of-Service (DoS) attacks	• Secure OTA (over-the-air) firmware updates • Strong authentication for access • AI anomaly detection for abnormal settings
Implantable Loop Recorders	• Patient data breaches • Alteration of cardiac monitoring data • Wireless hijacking leading to false readings	• Data encryption for storage and transmission • Secure logging and access monitoring • Periodic vulnerability testing
Bioelectronic Blood Pressure Regulators	• Unauthorized voltage modifications • AI-driven attacks manipulating treatment • Network compromise via hospital systems	• AI-based behavioural pattern monitoring • Segmented wireless communication • Secure firmware validation
Smart Cochlear Implants	• Audio interception • Firmware corruption • AI-driven misinformation in speech processing	• Secure AI integration for speech analysis • Embedded firewall mechanisms • AI-driven malware detection
Retinal Implants	• False image injection AI adversarial attacks altering vision • Exploiting image processing vulnerabilities	• Secure vision data encryption • AI-driven authentication for image integrity • Reinforced deep-learning security measures

Medical Digital Implant	**Possible Cyber Threats**	**Recommended Solutions**
Smart Insulin Pumps	• Unauthorized insulin delivery changes • Wireless disruption causing dosage miscalculations • API exploitation via hospital networks	• End-to-end encrypted insulin control • Secure API management • Continuous monitoring for anomalies
Gastric Stimulators	• Disrupting functionality via cyber-attacks • Wireless interference affecting treatment • Unauthorized access to data logs	• Encrypted signal transmission • Secure remote authentication • Periodic cybersecurity audits
Bionic Limbs and Prosthetics	• Neural hijacking causing movement disruption • AI adversarial attacks manipulating control • Unauthorized remote operation	• Secure AI command authentication • Embedded anti-malware software • Continuous anomaly detection AI models

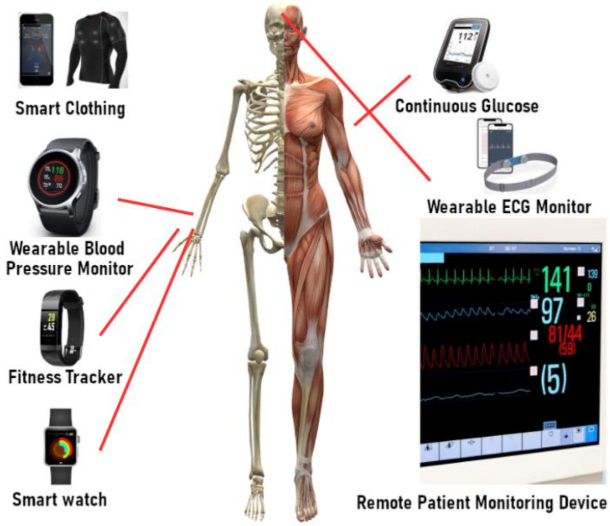

Figure 2: Medical Digital Wearable for Human Body

Figure 2 shows diagrammatic examples of a few popular medical digital wearable for human body. Refer to table 2 showing the popular medical digital wearable for the human body and possible cyber threats with recommended solutions [15, 16, 17, 18, 19, 20, 21, 22].

TABLE 2. MEDICAL DIGITAL WEARABLES FOR HUMAN BODY

Wearable Device	Possible Cyber Threats	Recommended Solutions
Smartwatches	• Data interception during transmission • Unauthorized access to health data	• Implement end-to-end encryption • Multi-factor authentication • Regular software updates
Fitness Trackers	• Weak app security leading to data breaches • GPS tracking vulnerabilities	• Secure app integrations • Disable GPS when not needed • Use strong encryption
Smart Rings	• IoT ecosystem vulnerabilities • Unauthorized access to sensitive data	• Strengthen IoT security protocols • Use secure boot mechanisms • Regular firmware updates
Continuous Glucose Monitors	• Manipulation of glucose data • Interception of real-time health data	• Encrypt data transmission • Secure cloud storage • Implement robust authentication
Wearable ECG Monitors	• Exploitation of communication protocols • Exposure of sensitive cardiac data	• Use secure communication channels • Regular patching • Strong credential management
Smart Clothing	• IoT vulnerabilities, unauthorized access to sensor data	• Implement secure IoT frameworks • Regular security audits • Strong encryption
Wearable Blood Pressure Monitors	• Data manipulation • Weak authentication mechanisms	• Use multi-factor authentication • Secure data storage • Regular security updates
Remote Patient Monitoring Devices	• Data breaches during transmission • Unauthorized access to patient data	• Encrypt data transfer • Secure cloud platforms • Implement strong access controls

The conventional surgical interface between a surgical instrument, a surgeon, and a patient has been revolutionized by robotic assisted surgery (RS). An improved three-dimensional view of the surgical field can now be obtained by a surgeon controlling robotic arms from a distance. Clinical benefits of RS have been demonstrated by research, including improved ergonomics that extend surgeons' careers and enhanced precision and postoperative complications. Its expense, lengthier operating times, and lack of haptic feedback for surgeons are still having concerns. According to recent research, in response to questions about having RS done by a physician who wasn't in the same room, hospital, or nation, participants' discomfort levels increased with distance [4].

TABLE 3. POSSIBLE CYBER THREATS FOR HEALTHCARE ROBOTICS SYSTEM

Attack Name	Description
Denial of Service (DoS)	Overwhelms the robot's network/system with excessive traffic, rendering it unable to respond to legitimate requests, delaying patient care.
Spoofing	An attacker impersonates a trusted entity to gain unauthorized access, leading to data breaches or manipulation of sensitive patient information.
Man-in-the-Middle Attack (MitM)	Intercepts communication between the robot and control system, altering or stealing transmitted data, compromising its confidentiality and integrity.
Tampering	Unauthorized modification of hardware/software, altering functionality and potentially leading to unsafe operations or incorrect diagnoses.
Replay Attacks	Captures and retransmits valid data packets to deceive the system into performing unauthorized actions, disrupting operations and safety.
Fault Injection Attack	Deliberately introduces faults to exploit vulnerabilities, manipulating behavior or extracting sensitive data, affecting reliability.
Sybil Attack	Creates multiple fake identities to manipulate the network, spreading misinformation or disrupting decision-making processes.
Jamming Attack	Disrupts wireless communication by overwhelming it with interference, causing delays or failures in transmitting critical data.
Hardware Backdoor Attack	Exploits hidden vulnerabilities in hardware to gain unauthorized access, compromising operations and exposing sensitive data.
Remote Access Trojan (RAT)	Allows attackers to remotely control the robot, stealing data, manipulating functions, or disabling the system entirely.
Stealthy Attack	Remains undetected while gradually extracting data or altering operations without raising alarms.
Homing Attack	Manipulates the robot's navigation system, causing it to deviate from its intended path, endangering patients or workflows.
Teardrop Attack	Exploits vulnerabilities by sending fragmented data packets that cannot be reassembled, leading to crashes or failures.
Phishing	Targets healthcare staff to reveal credentials or install malware, compromising the robot's security.
Hijacking	Attackers take control of the system, altering operations or using it as a gateway to access other critical systems.
Masquerade Attack	Stolen credentials are used to impersonate an authorized user, compromising functionality or sensitive data.

Contemporary robotics systems enable human-robot interaction in various settings. Robot safety is crucial, but focusing solely on safety may not guarantee secure applications. Extensive safety standards are needed as robots become more advanced. Robot capabilities and safety features are influenced by the environment in which they operate. Healthcare robot systems can undergo various cyber-attacks as shown in table 3. Also, the use of robotic systems in healthcare industry can increase vulnerabilities

listed below[5].
• Information disclosure and technical materials on manufacturer's website.
• Outdated software vulnerabilities due to custom patches.
• Default authentication through remote connections.
• Poor transport encryption due to HTTPS's lack of symmetric keys.
• Poor software protection through changes to software images on manufacturers' websites.
• Security by Obscurity due to inadequate information about robots.

Figure 3 reveals the typical cyber threat landscape for any healthcare SME, which consists of malware attacks, phishing attacks, insider threats, web attacks, and ransomware. These threats can be prevented through well-planned technical controls and cybersecurity awareness training. Strong guidelines, policies, technology controls, and physical controls can create a robust cybersecurity wall to protect an organization's assets.

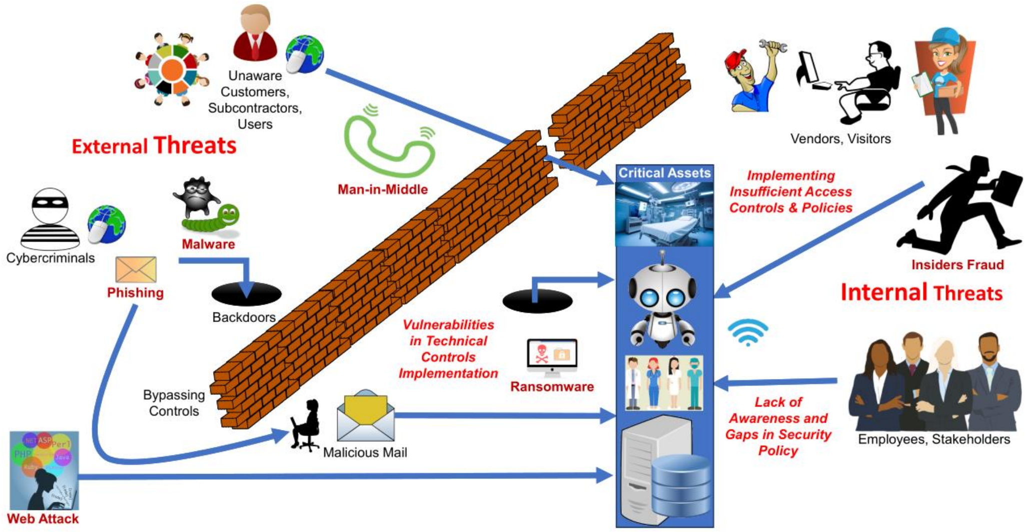

Figure 3: Typical Cyber Threats on Healthcare Industry

Figure 4 shows the latest statistics of ransomware attacks on healthcare industry based on cyber news. Three of the seven attacks in February 2025 were attributed to Medusa. Despite facing a $1 million ransom, SimonMed Imaging, a US company, claimed to have successfully "interrupted" hackers, preventing any encrypted data from being compromised. According to Medusa, 213 GB of data got stolen. After Medusa posted it on their website with a $2 million ransom after allegedly stealing nearly 2.3 TB of data, HCRG Care Group, UK, acknowledged that it had been attacked. Midway through February, Bell Ambulance, US, alerted staff members to a cyberattack. Medusa then demanded a $400,000 ransom for 212 GB of data. Mackay Memorial Hospital (Taiwan), LUP-Kliniken gGmbH (Germany), Genea (Australia), and Utsunomiya Central Clinic (Japan) are among the other organizations that were attacked in February. According to confirmed reports, the Utsunomiya Central Clinic breach affected 300,000 people, making it the largest healthcare breach this year (via ransomware). This attack was claimed by Qilin. To stop its attackers (Termite) and other parties from accessing, using, sharing, or making the stolen data public, Genea requested a court-ordered injunction. However, there are 29 attacks from January 2025 and 40 unconfirmed attacks from February 2025 [33].

As per the data reported by the Department of Human and Health Services, The USA to the congress, ePHI of 42 million individuals got affected in the year 2022 [36].

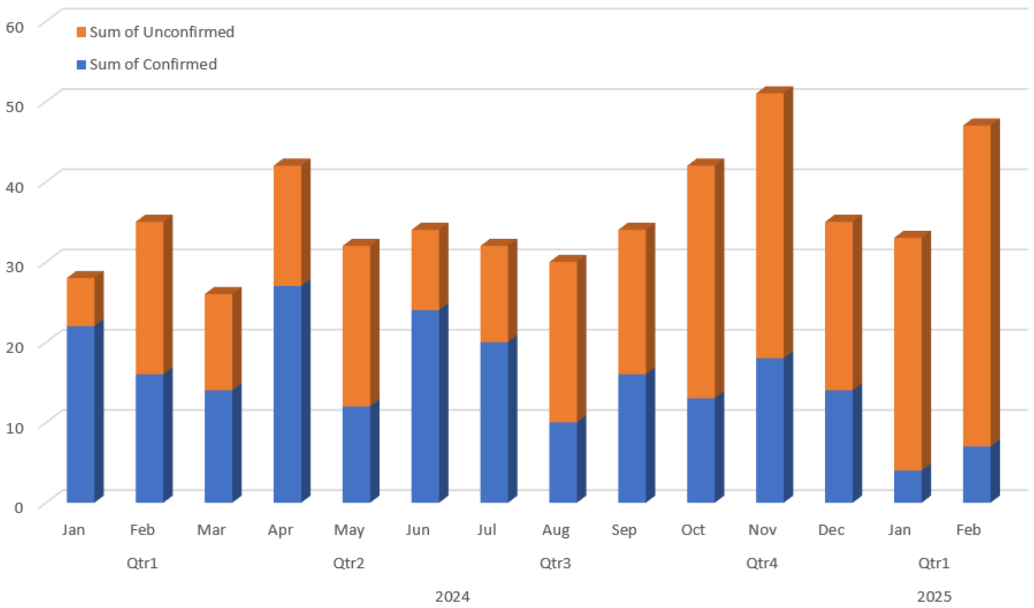

Figure 4: Latest Ransomware Attack Statistics on Healthcare Industry

3. RELATED WORK

The Health Insurance Portability and Accountability Act (HIPAA) , enacted in 1996 as a USA federal law, has evolved over time with the introduction of the Privacy Rule in 2003, the Security Rule in 2005, Enforcement Rule in 2006 and HIPAA Final Rule also known as Omnibus Rule in 2013 [23, 24, 25]. Organizations that handle electronic Protected Health Information (ePHI), such as health plans, healthcare clearinghouses, and healthcare providers, are subject to the HIPAA regulation in the United States. The organization's business processes and whether or not they handle ePHI determine the applicability of HIPAA. If an entity handles ePHI, even small businesses that sponsor group health plans or offer health-related services are required to abide by HIPAA. HIPAA rules must also be followed by business associates like contractors or vendors to health providers. Health plans, business associates, and healthcare providers handling ePHI are subject to the U.S.-specific HIPAA regulation. Strict reporting is required as per HIPAA for breaches of protected health information, especially when more than 500 individualsare involved. However, HIPAA's guidance does not effectively take care of increasing cyber security threats as security threats have evolved both in size as well as complexity since 2013, last date of HIPAA amendment [26]. U.S. Department of Health and Human Services (HHS), supervisory authority for HIPAA published a Notice of Proposed Rulemaking (NPRM) on 6 January 2025, which outlined potential updates to the HIPAA Security Rule though [36]. HIPAA Security Rule mandates administrative, physical, and technical safeguards to ensure confidentiality, integrity and availability of ePHI. Table 4 shows a few key highlights of HIPPA.

TABLE 4. OVERVIEW OF HIPPA

Area	Description
Objective	Ensures the security, confidentiality, and protection of electronic protected health information (ePHI).
Important Rules	• Privacy Rule: Governs the use and disclosure of ePHI. • Security Rule: Focuses on the protection of electronic ePHI with administrative, technical, physical safeguards and organizational requirements. • Breach Notification Rule: Requires notification to affected individuals, HHS and media in case of ePHI breaches. • Enforcement Rule: Establishes procedures for investigation, appeal, etc and penalties for non-compliance.
Covered Entities and Business Associates	Covered Entities include: • Healthcare Providers (e.g., hospitals, clinics, pharmacies), • Health Plans (e.g., insurance companies, government programs), • Healthcare Clearinghouses • Other than these organizations or individuals providing services to Covered Entities, such as IT providers, consultants, etc are categorized as Business Associates.
Key Compliance Requirements	• Conduct Risk Assessments • Implement safeguards for the protection of ePHI • Provide HIPAA awareness training for workforce • Ensure secure transmission and storage of ePHI • Enter into Business Associate Agreements (BAAs) with downstream service providers
Safeguards / Controls	• Administrative Safeguards: Policies, training, access control mechanisms. • Physical Safeguards: Facility access controls, workstations, and device security. • Technical Safeguards: Encryption, secure access, audit controls and resilience requirements for ePHI.
Penalties for Non-Compliance	Tiered penalties range from $100 to $1.5 million per violation, based on the level of negligence.
Breach Notification	• Notify affected individuals within 60 days of discovery. • Notify the Secretary, HHS and media if the breach affects more than 500 individuals within 60 days of discovery and Secretary, HHS within 60 days after the end of the calendar year if the breach affected less than 500 individuals.
Industries Affected	Healthcare providers, health IT companies, insurers, third-party administrators, and more.

SMEs in the healthcare industry are facing many barriers to implementing cybersecurity. According to the latest study on European healthcare SMEs, it is challenging for these businesses to completely mitigate the risks of cyberattacks due to their small workforce and restricted budgets. According to studies, healthcare SMEs do not prioritize cybersecurity because it is not a part of their primary business [12]. Adapting to changing legal and technological changes, managing compliance across multiple departments, and comprehending and applying complex regulations to particular business practices are just a few of the challenges that many organizations face [13].

During studies performed by Dr. Pawar by taking participation from SMEs of 19 different countries, it was evident that SMEs are facing three primary issues. Firstly, SMEs do not have enough financial budget available for implementing cybersecurity standards available in the market; secondly, these organizations do not employ skilled employees to implement and maintain cybersecurity controls; and thirdly, these organizations can not relate to what the return on investment (ROI) will be after investing in cybersecurity controls.

The Business Domain Specific Least Cybersecurity Controls Implementation (BDSLCCI) framework is a cybersecurity framework designed to help organizations, especially micro, small and medium enterprises (MSMEs), depending on region which are also known as small and medium enterprises (SMEs) or small and medium businesses (SMBs), prioritize and implement cybersecurity controls based on their specific business domains. BDSLCCI Framework provides a step-by-step approach to enhance an organization's cybersecurity posture by focusing on business-critical assets and operations. Mission Critical Asset (MCA) is the core asset vital to an organization's operations, such as critical operation computerized system, sensitive databases, software applications, or even digital infrastructure. For any hospital, Intensive Care Unit (ICU) equipment might be the first consideration of MCA. If a healthcare SME is dealing with human body implants or wearables, security best practices for those can be prioritized considering those as MCAs. Also, these SMEs need to examine manufacturers' and suppliers' cybersecurity policies to prevent vulnerabilities brought about by third-party components. BDSLCCI framework emphasizes identifying these assets and implementing specific controls to ensure their security, such as encryption, access control, and regular backups. Defense in Depth (DiD) is a layered security strategy that uses multiple defenses to protect against threats. If one layer fails, others remain active to mitigate risks [34]. BDSLCCI framework incorporates DiD by recommending security measures across various layers. As shown in figure 5, BDSLCCI framework considers both MCA and DiD controls.

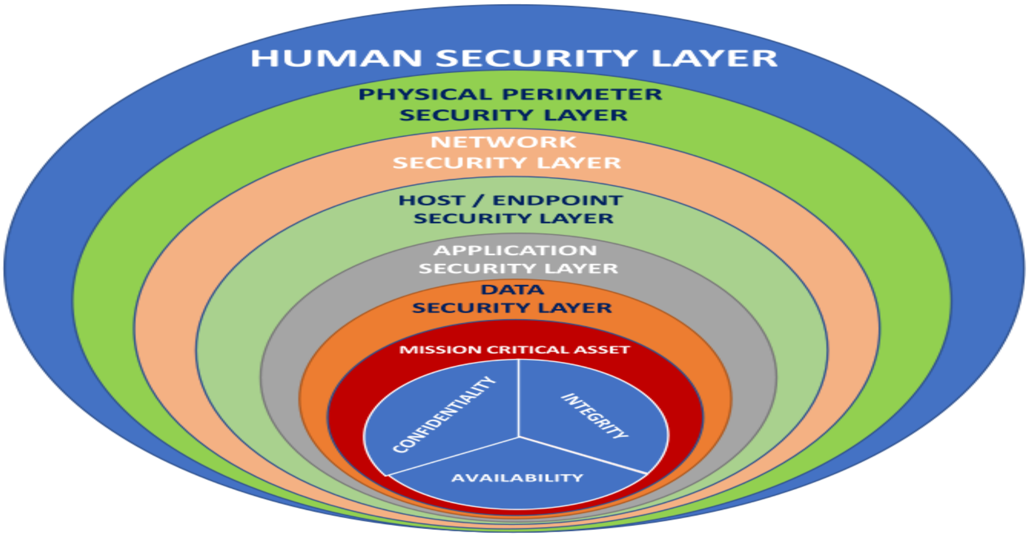

Figure 5: BDSLCCI Framework covering Defense in Depth (DiD) and MCA Cybersecurity Controls

Mission-critical assets in a hospital's cyberspace are crucial for patient care, operational continuity, and data security. These assets include Electronic Health Records (EHRs), medical devices, Hospital

Information Systems (HIS), communication systems, pharmacy systems, laboratory information systems, network infrastructure, and backup and recovery systems. EHRs store sensitive patient data, medical devices manage administrative tasks, communication systems facilitate real-time coordination among healthcare staff, pharmacy systems manage medication inventory and dispensing, and LIS handles diagnostic data and test results. Network infrastructure ensures secure connectivity, and backup and recovery systems provide data redundancy and disaster recovery to maintain operations during cyber incidents [31, 32]. In the case of the BDSLCCI framework, these assets can be protected by taking a prioritized approach for relative confidentiality, integrity, and availability.

Figure 6 outlines the Defense in Depth (DiD) layers as defined by the BDSLCCI framework. It categorizes cybersecurity controls into distinct layers, each addressing specific aspects of organizational security. These layers include host/endpoint security, data security, human security, network security, application security, and physical perimeter security. Each layer is further broken down into actionable control areas, such as endpoint protection, encryption, cybersecurity awareness training, network firewalls, application hardening, and physical access controls. This structured approach ensures a comprehensive and prioritized defense strategy, tailored to mitigate modern cyber threats effectively. The framework emphasizes practical implementation, particularly for small and medium-sized enterprises (SMEs), to enhance their cybersecurity posture systematically [27, 28, 29, 30].

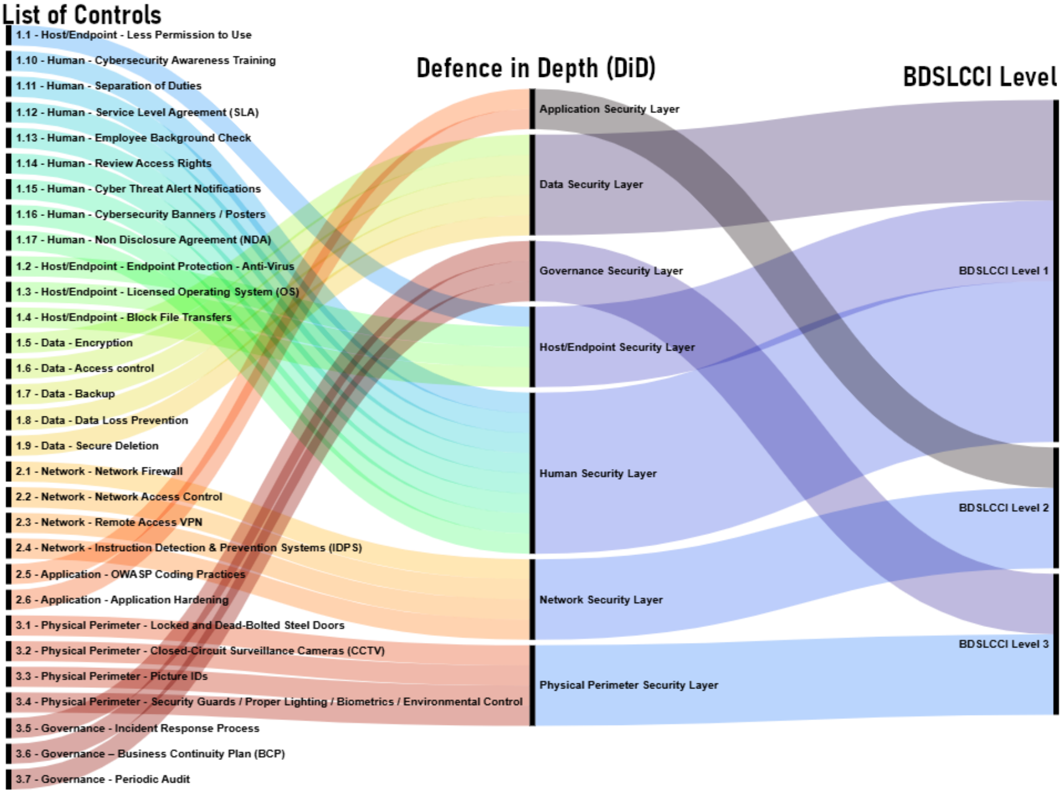
List of Controls
1.1 - Host/Endpoint - Less Permission to Use
1.10 - Human - Cybersecurity Awareness Training
1.11 - Human - Separation of Duties
1.12 - Human - Service Level Agreement (SLA)
1.13 - Human - Employee Background Check
1.14 - Human - Review Access Rights
1.15 - Human - Cyber Threat Alert Notifications
1.16 - Human - Cybersecurity Banners / Posters
1.17 - Human - Non Disclosure Agreement (NDA)
1.2 - Host/Endpoint - Endpoint Protection - Anti-Virus
1.3 - Host/Endpoint - Licensed Operating System (OS)
1.4 - Host/Endpoint - Block File Transfers
1.5 - Data - Encryption
1.6 - Data - Access control
1.7 - Data - Backup
1.8 - Data - Data Loss Prevention
1.9 - Data - Secure Deletion
2.1 - Network - Network Firewall
2.2 - Network - Network Access Control
2.3 - Network - Remote Access VPN
2.4 - Network - Instruction Detection & Prevention Systems (IDPS)
2.5 - Application - OWASP Coding Practices
2.6 - Application - Application Hardening
3.1 - Physical Perimeter - Locked and Dead-Bolted Steel Doors
3.2 - Physical Perimeter - Closed-Circuit Surveillance Cameras (CCTV)
3.3 - Physical Perimeter - Picture IDs
3.4 - Physical Perimeter - Security Guards / Proper Lighting / Biometrics / Environmental Control
3.5 - Governance - Incident Response Process
3.6 - Governance – Business Continuity Plan (BCP)
3.7 - Governance - Periodic Audit
Defence in Depth (DiD)
Application Security Layer
Data Security Layer
Governance Security Layer
Host/Endpoint Security Layer
Human Security Layer
Network Security Layer
Physical Perimeter Security Layer
BDSLCCI Level
BDSLCCI Level 1
BDSLCCI Level 2
BDSLCCI Level 3

Figure 6: BDSLCCI Framework covering detailed Defense in Depth (DiD) Controls

Three distinct levels of cybersecurity control form the components of the BDSLCCI. Levels 1 to 3 of BDSLCCI represent the foundational stages of cybersecurity maturity. Level 1 focuses on implementing the bare minimum cybersecurity controls to address critical vulnerabilities and protect essential assets. Level 2 builds upon this by introducing additional controls tailored to the organization's specific business domain, ensuring a stronger defense against common threats. Level 3 further enhances the cybersecurity posture by incorporating advanced measures and policies, fostering a more robust and resilient system. These levels are intended to be realistic and affordable, allowing SMEs to progressively enhance their cybersecurity without consuming excessive resources [29, 30].

4. BDSLCCI Framework Mapping with HAPPA related Control Areas

The BDSLCCI framework integrates cybersecurity controls within a DiD structure, ensuring a robust approach to organizational security while aligning with HIPAA Security Rule requirements (45 CFR § 164.3xx).This structured strategy categorizes controls into functions such as preventive, detective, corrective, deterrent, and recovery, distributing them across various layers like Host/Endpoint Security, Data Security, Human Security, Network Security, Application Security, Physical Perimeter Security, and Governance. Each control area is mapped to specific HIPAA Security Rule control provisions, covering aspects such as access control, transmission security, contingency planning, and workforce security. This ensures both comprehensive cybersecurity measures and compliance with regulatory standards, empowering organizations, especially in the healthcare sector, to address threats effectively while maintaining adherence to HIPAA Security Rule requirements. Refer table 5 for the BDSLCCI controls mapping with HIPPA related control areas [23, 24, 25, 26, 28, 29, 30, 34].

Table 5. BDSLCCI controls Mapping with hippa control areas

Control Type	Defense in Depth (DiD) Control Areas	Specific BDSLCCI Controls	Mapped HIPAA Control Area	HIPAA Security Rule Reference (all under 45 CFR §)

Preventive, Deterrent	Host/Endpoint Security	Less Permission to Use	Information Access Management	164.308(a)(3)(i),
				164.308(a)(4)(i)
				164.308(a)(4)(ii)(B)
				and

Preventive, Detective	Host/Endpoint Security	Endpoint Protection - Antivirus	Protection from malicious software	164.308(a)(5)(ii)(B),
Preventive, Corrective	Host/Endpoint Security	Licensed Operating System (OS)	No Direct Consideration	Not directly covered in HIPAA
Preventive, Detective, Deterrent	Host/Endpoint Security	Block File Transfers	Transmission Security	164.312€(1)
Preventive	Data Security Layer	Encryption	Transmission Security	164.312(e)(1), 164.312(e)(2)(ii)
Detective, Corrective	Network Security Layer	Intrusion Detection and Prevention Systems (IDPS)	Integrity	164.312(c)(1)

Detective, Preventive	Human Security Layer	Access Control Logs	Login Monitoring
			Audit controls
				164.308(a)(5)(ii)(C)
				164.312(b)

Control Type	**Defense in Depth (DiD) Control Areas**	**Specific BDSLCCI Controls**	**Mapped HIPAA Control Area**	**HIPAA Security Rule Reference (all under 45 CFR §)**
Detective, Corrective	Governance Layer	Periodic Audits	Evaluation	164.308(a)(8)
Deterrent, Preventive	Human Security Layer	Cybersecurity Awareness Training	Security Awareness Training	164.308(a)(5)(i), 164.308(a)(5)(ii)(A)
Deterrent	Human Security Layer	Cybersecurity Banners/Posters	Security Awareness and Training	164.308(a)(5)(ii)(A)
Deterrent, Preventive	Human Security Layer	Non-Disclosure Agreement (NDA)	Access Authorization (Indirectly)	164.308(a)(4)(ii)(B)

Deterrent, Preventive	Physical Perimeter Security Layer	Locked Doors	Physical Safeguards, Facility access controls	164.310(a)(1)
				164.310(a)(2)(iii)

Detective, Deterrent	Physical Perimeter Security Layer	CCTV Surveillance	Physical Safeguards, Facility access controls	164.310(a)(2)(ii)
Recovery, Preventive	Data Security Layer	Backup	Contingency Plan	164.308(a)(7)(ii)(A),

Recovery, Corrective	Governance Layer	Business Continuity Plan (BCP)	Contingency Plan	164.308(a)(7)(ii)(B),
				164.308(a)(7)(ii)(C)
				164.308(a)(7)(ii)(D)
				164.308(a)(7)(ii)€

Recovery, Detective	Governance Layer	Incident Response Process	Security Incident Procedures, Response and reporting	164.308(a)(6)(i), 164.308(a)(6)(ii),
Corrective, Preventive	Data Security Layer	Secure Deletion	No Direct Consideration	Part of HIPAA Privacy Rule
Corrective, Preventive	Application Security Layer	Application Hardening	No Direct Consideration	Not Mapped

BDSLCCI guidelines cover the proposed HIPAA Security Rule amendments as well, NPRM for the same has been published by HHS in the federal register on 6 Jan 2025 [35]. Refer Table 6 for the BDSLCCI controls mapping with the proposed key amendments to HIPAA Security Rule [23, 24, 25, 26, 28, 29, 30, 34, 35].

TABLE 6. BDSLCCI CONTROLS MAPPING WITH HIPPA SECURITY RULE AMENDMENTS

Proposed HIPAA Security Rule amendment (Only key changes included)	**HIPAA Security Rule Ref**	**Control Type**	**Defense in Depth (DiD) Control Areas**	**Specific BDSLCCI Controls**
Network map (Data Flow Diagram) of the ePHI to be maintained in addition to ePHI inventory	164.308(a)(1)	Corrective, Preventive, Recovery, Detective	Network Security Layer, Governance Layer	Network Segmentation, Asset Tracker, Access Control, BCP
Patch Management of electronic information systems	164.308(a)(4)	Corrective, Preventive, Recovery	Host/Endpoint Security Layer, Application Security Layer	Licensed Operating System (OS), Application Hardening, Application Regular Update Security Guidelines, Patch management Guidelines
Perform and document an audit at least once every 12 months	164.308(a)(14)	Corrective, Preventive, Deterrent, Detective	Governance Layer	Periodic Audit
Separate user identities from identities used for administrative and other increased access privileges.	164.312(a)(2)(ii)	Corrective, Preventive, Deterrent, Detective	Host/Endpoint Security Layer, Data Security Layer, Human Security Layer	Less Permission to Use, Block File Transfers, Access control, Review Access Rights, ARCSIK Matrix*, Asset Tracker
Deploy technical controls that disable or suspend the access of a user or technology asset to relevant electronic information systems after a reasonable and appropriate predetermined number of unsuccessful authentication attempts.	164.312(a)(2)(v)	Preventive, Deterrent, Detective	Host/Endpoint Security Layer, Human Security Layer, Data Security Layer, Network Security Layer, Application Security Layer, Governance Layer	Block File Transfers, Separation of Duties, ARCSIK Matrix, Data Loss Prevention, Network Firewall, OWASP** Coding Practices,

Proposed HIPAA Security Rule amendment (Only key changes included)	**HIPAA Security Rule Ref**	**Control Type**	**Defense in Depth (DiD) Control Areas**	**Specific BDSLCCI Controls**
				Application Hardening, Periodic Audit
Deploy technical controls to ensure that electronic information systems are segmented	164.312(a)(2)(vi)	Corrective, Preventive, Deterrent	Network Security Layer, Application Security Layer, Governance Layer	Network Segmentation, OWASP Coding Practices, Application Hardening, Periodic Audit
Configuration management of lectronic information systems	164.312©(1)	Corrective, Preventive, Deterrent, Detective	Network Security Layer, Application Security Layer, Governance Layer	Network Firewall, Network Access Control, Remote Access VPN, Instruction Detection and Prevention Systems (IDPS), OWASP Coding Practices, Application Hardening, Periodic Audit
Remove extraneous software from electronic information systems	164.312©(2)(ii)	Corrective, Preventive, Deterrent, Detective	Host/Endpoint, Governance Layer	Less Permission to User, Asset Tracker, Access Control, Application Regular Update Security Guidelines, Patch management Guidelines, Periodic Audit
Configure and secure operating system(s) and software	164.312©(2)(iii)	Corrective, Preventive	Host/Endpoint Security Layer, Application Security Layer, Governance Layer	Licensed Operating System (OS), Application Hardening,

Proposed HIPAA Security Rule amendment (Only key changes included)	HIPAA Security Rule Ref	Control Type	Defense in Depth (DiD) Control Areas	Specific BDSLCCI Controls
				Application Regular Update Security Guidelines, Patch management Guidelines, Asset Tracker, Periodic Audit
Disable network ports in accordance with risk analysis	164.312©(2)(iv)	Corrective, Preventive, Deterrent, Detective	Network Security Layer, Application Security Layer, Governance	Network Firewall, Network Access Control, Remote Access VPN, Instruction Detection and Prevention Systems (IDPS), OWASP Coding Practices, Application Hardening, Periodic Audit
Deploy multi-factor authentication to all technology assets in relevant eletronic information systems	164.312(f)(2)(ii)	Corrective, Preventive, Deterrent, Detective	Network Security Layer, Application Security Layer, Governance	Network Firewall, Network Access Control, Remote Access VPN, Instruction Detection and Prevention Systems (IDPS), OWASP Coding Practices, Application Hardening, Periodic Audit
Identify and address technical vulnerabilities including periodic VAPT	164.312(h)	Corrective, Preventive, Deterrent, Detective	Application Security Layer, Governance	OWASP Coding Practices, Application Hardening, Periodic Audit

Proposed HIPAA Security Rule amendment (Only key changes included)	**HIPAA Security Rule Ref**	**Control Type**	**Defense in Depth (DiD) Control Areas**	**Specific BDSLCCI Controls**
Data backup – RPO (Recovery Point Objective) should be less than 48 hours	164.312(i)(2)(i)	Corrective, Preventive, Recovery	Data Security Layer, Network Security Layer, Application Security Layer, Governance	Backup, Data Loss Prevention, Network Access Control, OWASP Coding Practices, Application Hardening, Periodic Audit
Review and test the effectiveness of such technical controls at least once every six months	164.312(j)	Corrective, Preventive, Deterrent, Detective	Application Security Layer, Governance	OWASP Coding Practices, Application Hardening, Periodic Audit

* *The ARCSIK matrix in the BDSLCCI framework is a tool designed to improve separation of duties within organizations. It consists of six roles:* ***Accountable, Responsible, Consulted, Supportive, Informed, and Knowledgeable.*** *Accountable is responsible for ensuring risks are managed,* ***R****esponsible for completing tasks,* ***C****onsulted provides direction and assistance,* ***S****upportive contributes to task planning and administration,* ***I****nformed is kept updated on risks, and* ***K****nowledgeable allows for tasks not assigned to specific colleagues to be completed by anyone with necessary expertise.*

** *The Open Worldwide Application Security Project (****OWASP****) provides industry-wide recognized Secure Coding Practices, offering a concise, technology-agnostic checklist to help developers build secure software. It aids in developing secure web applications, mobile applications, APIs, cloud applications, generative AI systems, and even software supply chains.*

For the healthcare industry, BDSLCCI's MCA can consider assets like ICU equipment, patient databases, robotic systems used for remote surgery, and so on. It can help to implement a comprehensive cybersecurity posture for a hospital or any SME working in the healthcare industry. There are few areas where BDSLCCI has partial coverage in reference to HIPAA compliance. BDSLCCI offers cybersecurity audits, but it does not provide a HIPAA-specific compliance audit framework that ensures adherence to all the regulatory requirements as of today. Also, HIPAA requires business associate agreements (BAAs) in specific format and breach notification procedure, which are additional than BDSLCCI guidelines. Yet those can be managed by the healthcare industry as additional administrative controls in addition to BDSLCCI to comply with other requirements of HIPAA not directly addressed in BDSLCCI. This approach ensures enhanced cyber protection at the same time meeting regulatory requirements with small incremental efforts.

5. Conclusion

The BDSLCCI framework offers healthcare SMEs or hospitals tailored and cost-effective approach to cybersecurity, addressing their unique challenges and resource constraints. By implementing domain-specific controls, it helps protect sensitive patient data, comply with requirement of regulations like HIPAA, and mitigates various cyber risks as an additional advantage. Its stepwise methodology ensures that healthcare SMEs can enhance their cybersecurity posture without overwhelming their budgets or operations, fostering trust and resilience in their digital practices.

In the future, this framework can be further developed to support healthcare industry beyond the SME category.

Funding

This research received no external funding.

Acknowledgments

This project received no external finance.

Declaration of Interest's Statement

The author declares that there are no conflicts of interest regarding the publication of this paper.

Research Contribution

Shekhar Pawar: Conceptualization, Methodology, Software, Validation, Formal Analysis, Investigation, Resources, Data Curation, Writing - Original Draft, Visualization, Project Administration. **Jaganathan T:** Writing - Review and Editing.

REFERENCES

1. Bekbolatova, M., Mayer, J., Ong, C.W. and Toma, M., 2024, January. Transformative potential of AI in healthcare: definitions, applications, and navigating the ethical landscape and public perspectives. In Healthcare (Vol. 12, No. 2, p. 125). MDPI.
2. Paul, S., Riffat, M., Yasir, A., Mahim, M. N., Sharnali, B. Y., Naheen, I. T., Rahman, A., & Kulkarni, A. (2021). Industry 4.0 Applications for Medical/Healthcare Services. Journal of Sensor and Actuator Networks, 10(3), 43. https://doi.org/10.3390/jsan10030043.
3. Abbou, B., Kessel, B., Ben Natan, M., Gabbay-Benziv, R., Dahan Shriki, D., Ophir, A., Goldschmid, N., Klein, A., Roguin, A. and Dudkiewicz, M., 2024. When all computers shut down: the clinical impact of a major cyber-attack on a general hospital. Frontiers in Digital Health, 6, p.1321485.
4. Brar, G., Xu, S., Anwar, M., Talajia, K., Ramesh, N. and Arshad, S.R., 2024. Robotic surgery: Public perceptions and current misconceptions. Journal of Robotic Surgery, 18(1), p.84.
5. Vallabhaneni, S., 2023. Research and Implement Solutions to Tackle Security Threats in Surgical Robotics.
6. Burke, W., Stranieri, A., Oseni, T. and Gondal, I., 2024. The need for cybersecurity self-evaluation in healthcare. BMC Medical Informatics and Decision Making, 24(1), p.133.
7. McGowan, A., Sittig, S. and Andel, T., 2021. Medical internet of things: a survey of the current threat and vulnerability landscape.
8. Gates, L., 2024. Cyber Attacks on Interoperable Electronic Health Records: A Clear and Present Danger. Missouri Medicine, 121(1), p.6.
9. Poongodi, R.K., Samuel, R., Rohith, P., Parthasarathy, S. and Ramana, B., 2024. Strengthening Cybersecurity in Indian Healthcare–Lessons from the Recent Ransomware Attacks on Hospitals.
10. ElSayed, Z., Abdelgawad, A. and Elsayed, N., 2025. Cybersecurity and Frequent Cyber Attacks on IoT Devices in Healthcare: Issues and Solutions. arXiv preprint arXiv:2501.11250.
11. van Boven, L.S., Kusters, R.W., Tin, D., van Osch, F.H., De Cauwer, H., Ketelings, L., Rao, M., Dameff, C. and Barten, D.G., 2024. Hacking acute care: a qualitative study on the health care impacts of ransomware attacks against hospitals. Annals of emergency medicine, 83(1), pp.46-56.
12. Walinga, J.P., 2024. Vigilant working with it at small medium enterprises in healthcare (Master's thesis, University of Twente).
13. Oyetunji, Semiu Adebayo (2024), Investigating Data Protection Compliance Challenges. International Journal of Innovative Science and Research Technology (IJISRT)

IJISRT24AUG1583, 2131-2147. DOI: 10.38124/ijisrt/IJISRT24AUG1583. https://www.ijisrt.com/investigating-data-protection-compliance-challenges

14. Catuogno, L. and Galdi, C., 2024. Implantable Medical Device Security. Cryptography, 8(4), p.53.
15. Longras, A., Pereira, T., Amaral, A. (2023). Cybersecurity Challenges in Healthcare Medical Devices. In: Pereira, T., Impagliazzo, J., Santos, H. (eds) Internet of Everything. IoECon 2022. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 458. Springer, Cham. https://doi.org/10.1007/978-3-031-25222-8_6
16. Tabasum, A., Safi, Z., AlKhater, W. and Shikfa, A., 2018, August. Cybersecurity issues in implanted medical devices. In 2018 International Conference on Computer and Applications (ICCA) (pp. 1-9). IEEE.
17. Ali, T.E., Ali, F.I., Dakić, P. et al. Trends, prospects, challenges, and security in the healthcare internet of things. Computing 107, 28 (2025). https://doi.org/10.1007/s00607-024-01352-4.
18. Mejía-Granda, C.M., Fernández-Alemán, J.L., Carrillo-de-Gea, J.M. et al. Security vulnerabilities in healthcare: an analysis of medical devices and software. Med Biol Eng Comput 62, 257–273 (2024). https://doi.org/10.1007/s11517-023-02912-0
19. Canali, S., Schiaffonati, V. and Aliverti, A., 2022. Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness. PLOS Digital Health, 1(10), p.e0000104.
20. Bouderhem, R. (2023). Privacy and Regulatory Issues in Wearable Health Technology. Engineering Proceedings, 58(1), 87. https://doi.org/10.3390/ecsa-10-16206
21. Boumpa, E., Tsoukas, V., Gkogkidis, A., Spathoulas, G., Kakarountas, A. (2022). Security and Privacy Concerns for Healthcare Wearable Devices and Emerging Alternative Approaches. In: Gao, X., Jamalipour, A., Guo, L. (eds) Wireless Mobile Communication and Healthcare. MobiHealth 2021. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 440. Springer, Cham. https://doi.org/10.1007/978-3-031-06368-8_2
22. ElSayed, Z., Abdelgawad, A. and Elsayed, N., 2025. Cybersecurity and Frequent Cyber Attacks on IoT Devices in Healthcare: Issues and Solutions. arXiv preprint arXiv:2501.11250.
23. Elkourdi, F., Wei, C., Xiao, L., Yu, Z. and Asan, O., 2024. Exploring Current Practices and Challenges of HIPAA Compliance in Software Engineering: Scoping Review. IEEE Open Journal of Systems Engineering.
24. Sadri, M., 2024. HIPAA: A Demand to Modernize Health Legislation. The Undergraduate Law Review at UC San Diego, 2(1).
25. Riad, A.K.I., Barek, M.A., Rahman, M.M., Akter, M.S., Islam, T., Rahman, M.A., Mia, M.R., Shahriar, H., Wu, F. and Ahamed, S.I., 2024, July. Enhancing HIPAA Compliance in AI-driven mHealth Devices Security and Privacy. In 2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 2430-2435). IEEE.
26. Tully, J., Selzer, J., Phillips, J.P., O'Connor, P. and Dameff, C., 2020. Healthcare challenges in the era of cybersecurity. Health security, 18(3), pp.228-231.
27. Pawar, S., & Palivela, H. (2025). Review and Design of Business Domain-Specific Cybersecurity Controls Framework for Micro, Small, and Medium Enterprises (MSMEs). Archives of Advanced Engineering Science, 1-19. https://doi.org/10.47852/bonviewAAES52024438.
28. Pawar, S. (2025). How BDSLCCI can Help SMEs to Achieve Data Protection Compliance, Such as EU GDPR and the DPDP Act of India. International Journal of Engineering Research & Technology, [online] 14(3). doi:https://doi.org/10.17577/IJERTV14IS030077.

29. Pawar, S.A. and Palivela, H. (2023). Importance of Least Cybersecurity Controls for Small and Medium Enterprises (SMEs) for Better Global Digitalised Economy. Contemporary Studies in Economic and Financial Analysis, [online] 110B(978-1-83753-417-3), pp.21–53. Available at: https://ideas.repec.org/h/eme/csefzz/s1569-37592023000110b002.html [Accessed 8 Mar. 2024].
30. Pawar, S. and Palivela, Dr.H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). International Journal of Information Management Data Insights, [online] 2(1), p.100080. doi:https://doi.org/10.1016/j.jjimei.2022.100080.
31. Kulkarni, R. and Kulkarni, S. (2021). Hospital Asset Management Using IoT and RFID. International Journal of Research in Engineering and Science (IJRES) ISSN, [online] 9(8), pp.2320–9356. Available at: https://www.ijres.org/papers/Volume-9/Issue-8/Series-6/A09080106.pdf.
32. Scalco, A. (2021) "Control Systems Cyber Security Reference Architecture (RA) for Critical Infrastructure: Healthcare and Hospital Vertical Example," The journal of critical infrastructure policy. Policy Studies Organization.
33. Moody, R. (2025). Ransomware roundup: Q1 2025. [online] Comparitech.com. Available at: https://www.comparitech.com/news/ransomware-roundup-q1-2025/.
34. Pawar, S. and Palivela, H. (2025). NEED OF PARADIGM SHIFT IN CYBERSECURITY IMPLEMENTATION FOR SMALL AND MEDIUM ENTERPRISES (SMES). International Journal of Cybersecurity Intelligence & Cybercrime, [online] 8(1). doi:https://doi.org/10.52306/2578-3289.1184.
35. FederalRegister.gov (2025). HIPAA Security Rule To Strengthen the Cybersecurity of Electronic Protected Health Information. [online] Federal Register. Available at: https://www.federalregister.gov/documents/2025/01/06/2024-30983/hipaa-security-rule-to-strengthen-the-cybersecurity-of-electronic-protected-health-information.