IRSHAD

International Journal of Cyber Law

Legal Liability for Cyber-Attacks on Connected Medical Device Networks

Amina Anam[1*] · **Zaheer Ahmad**[2] · **Ayesha Hameed**[3] · **Farzana Batool**[4] · **Abrar Khan**[5]

[1] Lahore Leads University, Lahore Pakistan
[2] COMSATS University Islamabad, Pakistan
[3] Government College University, Lahore, Pakistan
[4] Bahauddin Zakariya University, Multan, Pakistan
[5] University of Karachi, Karachi, Pakistan

* *aminanam1122@gmail.com*

ABSTRACT

Connected medical devices increasingly expose hospitals and patients to significant cybersecurity risks. Hackers can remotely access pacemakers, insulin pumps, and monitoring equipment directly. Current legal frameworks focus primarily on device safety rather than cybersecurity vulnerabilities. This research examines how legal liability should apply following cyber-attacks on networked medical devices. Manufacturers design devices prioritizing functionality while often neglecting robust cybersecurity protection measures. Hospitals similarly lack clear legal guidance regarding network security responsibilities and obligations. This study employs qualitative doctrinal analysis examining existing product liability and healthcare regulations. Findings reveal significant gaps between traditional liability frameworks and modern networked medical technology risks. This research proposes clearer liability standards addressing manufacturer and healthcare provider cybersecurity responsibilities. Such standards would strengthen patient protection while clarifying accountability across the healthcare technology chain. The study offers practical recommendations for regulators, manufacturers, and healthcare institutions. This framework addresses urgent gaps in patient safety and healthcare cybersecurity governance today.

Keywords:*Medical Device Cybersecurity, Product Liability, Healthcare Regulation, Patient Safety, Connected Devices, Cyber-Attack Liability, Regulatory Compliance*

HOW TO CITE THIS ARTICLE (APA 7th Edition)

Anam, A.,Ahmad, Z., Hameed, A., Batool, F., &Khan,A. (2026). Legal Liability for Cyber-Attacks on Connected Medical Device Networks.*International Journal of Cyber Law*, 1(1), 31–45. https://doi.org/10.59022/iijcl.005

I. INTRODUCTION

Hospitals now connect thousands of medical devices directly to internet networks daily. Hackers can remotely access these devices, threatening patient safety directly. Pacemakers, insulin pumps, and monitors face growing cybersecurity vulnerabilities constantly. Current medical device laws focus primarily on safety and efficacy standards. These laws rarely address cybersecurity risks or resulting patient harm liability. Manufacturers design devices prioritizing functionality over robust cybersecurity protection measures. Hospitals similarly lack clear legal guidance regarding network security responsibilities. This gap leaves patients vulnerable while responsible parties avoid meaningful legal accountability. Courts struggle applying traditional product liability frameworks to networked medical technology. Regulators increasingly recognize cybersecurity as essential to overall medical device safety. This research examines how legal liability should apply to connected device attacks. It explores whether manufacturers, hospitals, or both bear primary legal responsibility. Clarifying this liability remains essential for protecting patients from cyber-enabled medical harm. The following sections examine this urgent and evolving legal and medical question (AllahRakha, 2026).

The devices historically functioned as standalone tools without network connectivity requirements. Manufacturers designed early devices focusing exclusively on mechanical safety and clinical effectiveness. Modern healthcare increasingly relies on networked devices sharing data across hospital systems. This connectivity improves patient monitoring but simultaneously creates significant new security vulnerabilities. Legal frameworks developed decades ago never anticipated these networked cybersecurity risks specifically. Product liability law traditionally addresses manufacturing defects rather than cybersecurity vulnerabilities directly. Healthcare regulation similarly focuses on clinical safety rather than digital security requirements. Scholars have studied medical device regulation extensively but rarely examined cybersecurity liability specifically. Few researchers connect device cybersecurity vulnerabilities directly to potential legal liability standards. This gap leaves courts without clear guidance addressing modern networked device realities. Existing laws fail distinguishing between traditional device defects and cybersecurity related harm. This distinction matters significantly for determining appropriate liability allocation frameworks today. This study addresses this gap by examining cybersecurity responsibility within liability frameworks (Javaid et al., 2023).

Connected medical devices currently operate within outdated liability and regulatory frameworks. These frameworks assume devices function safely without considering ongoing cybersecurity vulnerability management. Modern devices require continuous software updates addressing newly discovered security vulnerabilities regularly. This requirement contradicts traditional liability models focused on point-of-sale product safety. Existing laws provide no clear standard determining manufacturer responsibility for post-sale cybersecurity updates. Courts struggle applying outdated frameworks to devices requiring ongoing cybersecurity maintenance obligations. Patients harmed by cyber-attacks often lack effective legal remedies against manufacturers or hospitals. This gap leaves individuals vulnerable while responsible parties avoid meaningful cybersecurity accountability. Current research addresses medical device regulation broadly but rarely examines cybersecurity liability specifically. This research defines the exact problem as unclear liability standards for device cyber-attacks. It examines how liability should apply between manufacturers and healthcare institutions. It also explores what legal standards could establish ongoing cybersecurity maintenance duties. This study identifies specific criteria for allocating liability based on cybersecurity practices (Freyer et al., 2024).

Recent studies show medical device cybersecurity incidents increased significantly between 2020 and 2024. Researchers found hospital networks increasingly vulnerable to ransomware and device manipulation attacks. Scholars identified weak cybersecurity standards as a significant patient safety vulnerability. Legal experts noted courts struggle applying traditional product liability standards to cybersecurity harm. Studies revealed manufacturers often delay releasing critical security patches for older devices. Comparative research found different countries adopting varying approaches toward medical device cybersecurity regulation. Analysts observed regulatory agencies moving slowly compared to rapidly evolving cybersecurity threats. Legal scholars documented increasing patient advocacy demanding stronger device cybersecurity accountability standards. Researchers highlighted software vulnerability disclosure as a growing concern among manufacturers and regulators. Studies from recent years showed hospitals often lack resources implementing adequate network security. Scholars called for updated legal frameworks addressing ongoing device cybersecurity maintenance responsibilities. These findings collectively reveal significant gaps between existing law and device security practices (Menon, 2026).

Additional research examined specific regulatory attempts addressing medical device cybersecurity requirements directly. Findings showed some countries introduced mandatory cybersecurity standards for new

medical devices. Scholars studying comparative regulations found inconsistent approaches across different healthcare regulatory systems. Legal studies revealed enforcement mechanisms often lack sufficient authority ensuring manufacturer compliance. Researchers analyzing recent data found older devices remain particularly vulnerable to cyber-attacks. Legal scholars proposed treating cybersecurity maintenance as an ongoing manufacturer safety obligation. Studies on hospital cybersecurity found limited budgets restrict adequate network security investment. Analysts noted smaller healthcare facilities face different challenges compared to large hospital systems. Recent scholarship suggested creating shared liability frameworks between manufacturers and healthcare institutions. Legal researchers found existing case law provides limited guidance for device cybersecurity questions. Studies emphasized supply chain vulnerabilities complicate securing devices from multiple component manufacturers. Scholars argued current frameworks fail protecting patients from cybersecurity related medical device harm (McDermott et al., 2022).

Existing literature identifies medical device cybersecurity as a significant patient safety concern. Most research focuses broadly on device regulation without examining cybersecurity liability specifically. Few studies propose concrete criteria allocating liability between manufacturers and healthcare institutions. Scholars have documented growing cybersecurity vulnerabilities but rarely proposed detailed liability frameworks. Comparative studies highlight regulatory differences but lack unified standards applicable across jurisdictions. Researchers have examined vulnerability disclosure without connecting it directly to liability allocation. This gap prevents courts from developing consistent standards for device cybersecurity cases. Existing frameworks fail addressing how ongoing maintenance duties should influence liability determination. Future research must integrate cybersecurity practice analysis with formal legal liability criteria. This study fills that gap through detailed liability allocation framework analysis. It proposes specific criteria connecting cybersecurity practices to legal accountability standards directly. This approach bridges fragmented research areas into a coherent liability framework (Williams et al., 2015).

To examine how cybersecurity vulnerabilities in connected medical devices challenge traditional product liability frameworks.

To identify specific criteria allocating liability between manufacturers and healthcare institutions for cyber-attacks.

To propose a legal framework establishing ongoing cybersecurity maintenance responsibilities for medical device manufacturers.

How should legal liability be allocated between manufacturers and healthcare institutions following cyber-attacks on connected medical devices?

The device cybersecurity failures carry significant consequences for patients and healthcare institutions broadly. This research holds substantial value for legal scholars, regulators, and healthcare policymakers globally. It addresses a critical gap between medical device liability law and cybersecurity realities. Courts will benefit from clearer criteria allocating liability between manufacturers and healthcare providers. Policymakers can use this framework designing updated medical device cybersecurity regulations effectively. Patients harmed by cyber-attacks will gain stronger legal grounds for seeking remedies. Manufacturers will receive clearer guidance regarding ongoing cybersecurity maintenance legal obligations. This study contributes new knowledge connecting cybersecurity practices with formal liability standards. It offers a fresh legal perspective absent from most existing academic literature. Regulators can use these findings crafting proportionate cybersecurity compliance requirements for manufacturers. Healthcare institutions will benefit from clearer network security responsibility guidance and standards. This work ultimately strengthens patient safety while clarifying healthcare technology accountability structures. It provides a foundation for future research examining healthcare cybersecurity liability reform (Conceição et al., 2026).

II. METHODOLOGY.

This research follows a qualitative research design suited for legal and healthcare policy analysis. Qualitative methods allow deep examination of laws, regulations, and healthcare cybersecurity standards. This study focuses on doctrinal analysis examining existing product liability and medical device frameworks. The population for this research includes global laws addressing medical device cybersecurity standards. The sample includes specific regulations, healthcare cybersecurity guidelines, and product liability statutes. This research analyzes laws related to medical device safety and cybersecurity maintenance obligations. Relevant frameworks include medical device regulations, healthcare data security laws, and product liability statutes. Data collection relies on scholarly literature, legal statutes, and regulatory guidance documents available publicly. Specific keywords guided this search, including medical device cybersecurity, product liability, and healthcare regulation. Additional keywords included connected device security,

cyber-attack liability, and healthcare technology governance. These keywords helped identify relevant scholarly articles, case law, and regulatory materials effectively.

This research retrieved legal materials directly from official government and regulatory websites. Scholarly articles were retrieved from established academic databases containing peer-reviewed legal research. This study prioritized recent publications, generally not exceeding five years old. Recent sources ensure this research reflects currently applicable laws and regulations. Materials were selected based on relevance to medical device cybersecurity and liability topics. Authors were evaluated based on academic credentials, institutional affiliation, and publication history. This research favored peer-reviewed articles published within recognized legal and healthcare journals. Sources were assessed based on citation frequency and use by other researchers. Official regulatory documents were treated as primary sources carrying authoritative legal weight. This approach ensured the research maintained strong academic validity and reliability standards.

Data analysis relied primarily on doctrinal analysis examining statutes, regulations, and legal principles. This research also employed document analysis examining scholarly articles and policy papers. Doctrinal analysis helped identify gaps, inconsistencies, and contradictions within existing legal frameworks. This research maintained strict ethical standards throughout the entire research process. Only publicly available official documents and scholarly materials were used throughout. Every scholarly article referenced received proper citation acknowledging original authors and their contributions. This research maintained no conflicts of interest throughout the entire research process. The study addresses several important limitations affecting overall conclusions and generalizability. Cybersecurity technology continues evolving rapidly, creating challenges predicting long-term legal relevance. Medical device regulations also change frequently, potentially affecting the applicability of specific findings. These limitations suggest conclusions should be understood within a specific evolving legal context. Delimitations include focusing specifically on cybersecurity liability rather than broader device safety issues.

III. RESULTS

This research examined how legal liability should apply to connected medical device cyber-attacks. Six distinct results emerged from analyzing current medical device liability and regulatory frameworks. These results directly answer the research question about manufacturer and institution accountability. Each finding highlights specific weaknesses within existing medical device liability legal standards. The analysis reveals significant gaps between traditional product liability assumptions and networked device realities. It also exposes inconsistent regulatory approaches across different healthcare cybersecurity jurisdictions globally. Furthermore, the findings demonstrate limited legal remedies available for patients harmed by cyber-attacks. Insufficient cybersecurity maintenance obligations prevent adequate long-term device security management currently. Unclear liability allocation between manufacturers and hospitals complicates accountability following security incidents. Weak regulatory enforcement mechanisms further complicate ensuring adequate device cybersecurity compliance broadly. These results collectively support establishing clearer liability standards based on cybersecurity practice quality. This clarity would strengthen accountability, patient safety, and healthcare cybersecurity governance significantly. The following results present detailed findings addressing these identified regulatory and legal gaps (AllahRakha, 2025).

Traditional product liability law focuses on defects existing at the point of sale. Medical devices require continuous cybersecurity updates addressing newly discovered vulnerabilities over time. This ongoing requirement contradicts liability frameworks designed around one-time manufacturing defect assessment. Manufacturers currently face no clear legal duty maintaining security support after initial sale. This absence allows companies discontinuing critical security patches without meaningful legal consequence. Hospitals continue operating devices assuming manufacturers will address newly discovered vulnerabilities promptly. This assumption often proves incorrect, leaving networked devices exposed to known security risks. Courts applying traditional liability standards find no clear basis for post-sale claims. Patients harmed by unpatched vulnerabilities struggle establishing manufacturer liability under existing legal doctrine. This gap creates a dangerous mismatch between technological reality and legal accountability. Recognizing ongoing cybersecurity maintenance as a manufacturer duty would close this significant gap. Such recognition would align legal responsibility with the genuine operational needs of connected medical technology (Petrov et al., 2025)..

Manufacturers design devices while hospitals manage network security and device deployment decisions. Current law provides no clear standard dividing cybersecurity responsibility between these two parties. This ambiguity complicates determining appropriate liability following successful cyber-attacks on medical devices. Manufacturers

argue that hospitals bear responsibility for network-level security configuration and monitoring. Hospitals counter that manufacturers bear responsibility for device-level vulnerabilities and design weaknesses. This disagreement leaves courts without clear guidance allocating liability between the two parties. Patients harmed by cyber-attacks face significant uncertainty regarding which party to pursue legally. This uncertainty discourages legitimate claims and complicates settlement negotiations following security incidents. Some incidents involve failures spanning both device design and hospital network configuration simultaneously. This overlap further complicates fair and accurate liability determination in individual cases. Establishing clearer division of responsibility would reduce this uncertainty considerably for all parties. Such clarity would also encourage both manufacturers and hospitals investing more consistently in cybersecurity (Ludvigsen et al., 2023).

Patients suffering harm from compromised medical devices currently lack effective legal remedies. Courts struggle applying traditional medical malpractice or product liability theories to cybersecurity harm. This gap leaves patients without meaningful accountability mechanisms following device security failures. Malpractice frameworks assume clinical error by treating physicians rather than external cyber intrusion. Product liability frameworks assume manufacturing defects rather than exploited software vulnerabilities specifically. Neither framework comfortably accommodates harm resulting from deliberate third-party cyber-attacks on devices. Patients pursuing claims face significant evidentiary challenges proving the precise cause of harm. Litigation costs frequently exceed potential recovery, discouraging patients from pursuing legitimate claims altogether. This financial barrier compounds the doctrinal gap, leaving many victims without practical recourse. Some patients have attempted novel legal theories, achieving limited and inconsistent success. These attempts highlight genuine structural gaps within existing healthcare and product liability law. Addressing this gap requires recognizing cybersecurity harm as a distinct, compensable category of injury (Jubaidi et al., 2025).

Regulatory agencies primarily evaluate device safety before market approval rather than ongoing security. Few regulations require manufacturers maintaining cybersecurity support throughout a device's operational lifespan. This gap leaves older devices particularly vulnerable to newly discovered cybersecurity threats. Approval processes focus heavily on clinical safety testing conducted before initial market release. These processes rarely address how manufacturers will manage vulnerabilities discovered after devices ship. Hospitals often continue using older devices for many years beyond their expected lifespan. Manufacturers frequently discontinue security support for these older devices without regulatory objection. This discontinuation leaves hospitals operating vulnerable equipment without adequate protective regulatory oversight. Some regulators have begun exploring lifecycle-based cybersecurity requirements addressing this specific gap. These exploratory efforts remain preliminary and inconsistently applied across different regulatory jurisdictions. Establishing mandatory lifecycle cybersecurity standards would meaningfully address this significant regulatory shortfall. Such standards would better protect patients relying on medical devices throughout their extended operational lives (Ostermann et al., 2025).

Medical devices often incorporate components and software from multiple different suppliers globally. This complexity complicates determining which party bears responsibility for specific cybersecurity vulnerabilities. Courts struggle allocating liability across complex multi-party medical device supply chains effectively. A vulnerability might originate in a chip, a software library, or the final assembly. Tracing responsibility through this layered structure requires substantial technical and legal investigation. Manufacturers often lack complete visibility into the security practices of upstream component suppliers. This limited visibility complicates manufacturers' ability preventing vulnerabilities embedded within purchased components. Component suppliers, meanwhile, face little direct legal exposure despite contributing to eventual device vulnerabilities. This mismatch between technical contribution and legal accountability creates troubling gaps in oversight. Some industry groups have proposed voluntary supply chain security verification standards for manufacturers. These voluntary efforts remain inconsistently adopted and lack meaningful enforcement mechanisms currently. Addressing this complexity requires legal frameworks that can trace liability across multi-party manufacturing relationships (Williams et al., 2015).

Regulators possess limited authority enforcing ongoing cybersecurity compliance among medical device manufacturers. This weakness allows manufacturers deprioritizing cybersecurity investment without facing meaningful regulatory consequences. Stronger enforcement mechanisms would incentivize manufacturers maintaining robust ongoing device security practices. Current enforcement tools often rely on voluntary manufacturer reporting rather than independent regulatory verification. This reliance allows manufacturers controlling the flow of information regulators use for oversight. Some regulatory agencies also lack sufficient technical staff evaluating complex cybersecurity compliance claims. This expertise shortage further weakens practical enforcement even where legal authority technically exists. Penalties for non-compliance, where they exist, often remain too modest deterring meaningful behavioral change. Manufacturers may treat these penalties as a manageable cost rather than a genuine

deterrent. Recent cybersecurity incidents have prompted some regulators reconsidering the adequacy of existing enforcement tools. These reconsiderations suggest growing recognition that current mechanisms remain insufficient for genuine accountability. Strengthening enforcement authority and resources remains essential for translating cybersecurity standards into real compliance (Ludvigsen, 2023).

IV. DISCUSSION

A.Outdated Product Liability Standards Ignore Ongoing Cybersecurity Maintenanc

This finding shows product liability law has not kept pace with device technology. Traditional standards evaluate defects existing when manufacturers first sell medical devices. Modern connected devices require continuous security updates addressing vulnerabilities discovered after sale. This ongoing need contradicts liability frameworks built around single-point defect assessment. Courts continue applying outdated standards without examining post-sale cybersecurity maintenance obligations. This oversight allows manufacturers escaping accountability despite neglecting known security vulnerability patches. Recent hospital ransomware incidents highlight consequences resulting from inadequate device security maintenance. Some regulators have proposed requiring manufacturers maintaining cybersecurity support throughout device lifespans. However, comprehensive legal reform addressing ongoing maintenance obligations remains largely absent currently. This gap leaves courts applying frameworks poorly suited to networked medical technology. Recognizing ongoing maintenance as a manufacturer duty would better reflect genuine safety needs. This recognition forms the foundation for meaningful liability reform moving forward significantly (Gennari, 2025).

This outdated framework produces serious practical consequences for patient safety and accountability. Without recognizing ongoing duties, manufacturers avoid responsibility for delayed security patch releases. Patients suffer harm while manufacturers claim their original product met applicable safety standards. This claim increasingly rings hollow given devices require continuous security maintenance afterward. Companies reduce costs by minimizing ongoing cybersecurity support for older device models. Yet liability frameworks fail connecting this cost-cutting behavior to resulting patient harm. Updating liability standards would align manufacturer responsibility with genuine device security needs. Manufacturers would then face meaningful incentives maintaining robust ongoing cybersecurity support programs. This shift could substantially reduce successful cyber-attacks against vulnerable medical devices. Patients would benefit from manufacturers treating cybersecurity as a continuing safety obligation. This continuing obligation remains central to protecting patients using connected medical technology.

Specific examples illustrate why outdated liability standards fail addressing modern device realities. Several hospital networks suffered ransomware incidents traced to unpatched, known device vulnerabilities. Investigations revealed manufacturers had known about certain vulnerabilities for extended periods beforehand. Despite this knowledge, courts dismissed related claims citing traditional point-of-sale liability standards. This pattern repeated across multiple incidents involving different manufacturers and device categories. Some lawmakers responded proposing legislation specifically addressing ongoing device security maintenance duties. These proposals reflect growing recognition that current standards remain fundamentally inadequate today. Several regulatory bodies have begun requiring vulnerability disclosure as a precursor to reform. These developments suggest momentum building toward eventually updating outdated liability frameworks meaningfully. However, comprehensive reform connecting disclosure requirements to actual liability remains still developing. This evidence strengthens arguments supporting formal recognition of ongoing maintenance as a legal duty.

This analysis acknowledges certain limitations regarding product liability reform research and conclusions. Legal traditions vary significantly across countries regarding manufacturer liability and consumer protection. Some jurisdictions maintain stronger manufacturer accountability traditions than others currently do. This variation complicates creating universally applicable ongoing maintenance liability recommendations globally. Additionally, cybersecurity technology continues evolving rapidly, complicating efforts creating fixed legal definitions. Standards developed today may struggle addressing future cybersecurity technology developments effectively. Furthermore, distinguishing reasonable maintenance efforts from negligent neglect remains technically challenging currently. Courts may lack sufficient technical expertise evaluating manufacturer cybersecurity maintenance practices accurately. These limitations suggest reform efforts must remain flexible and technically informed throughout. Legal reform must balance accountability goals against legitimate manufacturer cost and feasibility concerns. These considerations complicate but do not eliminate the need for meaningful reform.

Comparing liability approaches across jurisdictions reveals interesting contradictions worth examining closely. Some jurisdictions assume traditional point-of-sale liability adequately protects patients from device harm. Evidence increasingly suggests this assumption ignores the genuine ongoing nature of cybersecurity risk. Other jurisdictions have begun extending liability toward ongoing manufacturer maintenance obligations specifically. This divergence creates inconsistent global standards for essentially similar networked medical technologies. Some regulators assume market competition alone will encourage voluntary ongoing security investment. Evidence suggests competitive pressures often favor cost reduction over sustained cybersecurity investment instead. This contradiction challenges assumptions that market forces alone ensure responsible manufacturer behavior. These conflicting approaches demonstrate why voluntary industry practices remain fundamentally insufficient currently. Consistent legal standards recognizing ongoing maintenance would reduce these regulatory inconsistencies significantly. This comparison strengthens the case for coordinated international product liability reform efforts.

These findings carry substantial implications for lawmakers, regulators, and medical device manufacturers broadly. Legislators should consider updating product liability standards explicitly addressing ongoing cybersecurity maintenance. Regulators would benefit from clearer authority requiring manufacturers maintaining device security support. Manufacturers would gain clearer expectations guiding responsible long-term cybersecurity investment decisions. This clarified framework offers practical applicability across legislative, regulatory, and corporate governance contexts. Healthcare institutions could design procurement policies favoring manufacturers with strong security maintenance records. Patients would benefit from stronger legal grounds pursuing claims following inadequate security maintenance. Policymakers should prioritize this reform given growing healthcare reliance on connected medical devices. This research provides meaningful groundwork supporting future product liability reform development efforts. Legal reclassification directly addresses this outdated framework through updated ongoing maintenance accountability standards (Schorr et al., 2024).

B.Unclear Division of Cybersecurity Responsibility Between Manufacturers and Hospitals

These finding highlights genuine confusion regarding cybersecurity responsibility division within healthcare technology. Manufacturers control device design while hospitals control network configuration and deployment decisions. Current legal frameworks fail clearly assigning cybersecurity responsibility between these two distinct parties. This ambiguity produces inconsistent outcomes when courts evaluate liability following cyber-attacks. Some courts emphasize manufacturer design responsibility while others emphasize hospital network security duties. This inconsistency creates unpredictable legal outcomes across similar medical device cybersecurity cases. Hospitals and manufacturers both possess plausible arguments shifting responsibility toward the other party. This dynamic complicates establishing accountability regardless of which party bears greater practical fault. Recent policy discussions have emphasized needing clearer statutory frameworks dividing cybersecurity responsibility. Some jurisdictions have proposed shared liability models reflecting joint manufacturer and hospital roles. However, comprehensive and widely accepted division frameworks remain largely absent currently. This gap leaves fundamental accountability questions unresolved despite significant patient safety stakes (Aldosari, 2025).

This unclear division produces meaningful consequences affecting both patient safety and institutional accountability. Without clear division, both parties may underinvest in cybersecurity, assuming the other bears responsibility. This diffusion of responsibility creates dangerous gaps in overall device network security. Patients suffer harm from cybersecurity failures that neither party feels fully accountable preventing. Hospitals may deploy devices without adequately verifying manufacturer cybersecurity support commitments beforehand. Manufacturers may design devices assuming hospitals will implement adequate independent network protections. This mutual assumption creates dangerous gaps where genuine cybersecurity investment often falls short. Clear division would eliminate this diffusion, assigning specific responsibilities to each party explicitly. Hospitals would then know their specific network security obligations independent of manufacturer actions. Manufacturers would similarly understand their specific device-level cybersecurity maintenance responsibilities clearly. Establishing this clarity remains essential for closing dangerous cybersecurity responsibility gaps effectively.

Specific examples illustrate how unclear division produces inconsistent accountability outcomes in practice. Several hospital cyber incidents involved both outdated device firmware and weak network segmentation simultaneously. Investigations struggled attributing primary fault between manufacturer design and hospital network management. Litigation in some cases dragged on for years without clear liability resolution emerging. This prolonged uncertainty harmed patients awaiting compensation and institutions seeking clear future guidance. Some jurisdictions have experimented with joint liability models distributing responsibility between both parties. These experiments

show promise though comprehensive adoption remains limited across most legal systems. Industry groups have proposed voluntary responsibility-sharing agreements between manufacturers and healthcare institutions. These voluntary agreements lack the consistency and enforceability that formal legal standards would provide. This evidence demonstrates why clearer statutory division remains urgently needed for meaningful accountability.

This analysis acknowledges important limitations regarding responsibility division research and policy recommendations. Healthcare systems vary significantly in structure, resources, and technical sophistication across countries. This variation complicates designing universally applicable responsibility division standards for manufacturers and hospitals. Additionally, specific device types may require different division approaches given varying technical characteristics. Implanted devices differ substantially from networked monitoring equipment in their operational risk profiles. This diversity complicates creating a single, universally applicable division framework across device categories. Furthermore, hospitals vary considerably in their technical capacity managing sophisticated network security independently. Smaller facilities may lack resources that larger academic medical centers can readily deploy. These limitations suggest responsibility division frameworks must remain flexible and appropriately calibrated. Division standards should account for institutional capacity alongside baseline manufacturer design obligations.

Comparing responsibility models across different healthcare systems reveals interesting contradictions worth examining. Some systems assume manufacturers should bear primary responsibility given their specialized technical expertise. Other systems assume hospitals should bear primary responsibility given their direct network control. This disagreement reflects genuine uncertainty regarding which party possesses greater practical control. Some scholars argue shared liability models better reflect the genuinely collaborative nature of deployment. Others argue shared models create diffuse accountability that ultimately protects neither party adequately. This tension demonstrates why simplistic single-party liability models likely prove insufficient. Some jurisdictions favor contractual risk allocation between manufacturers and hospitals through procurement agreements. Other jurisdictions prefer mandatory statutory division independent of private contractual arrangements. This philosophical difference complicates achieving consistent approaches toward dividing cybersecurity responsibility internationally.

These findings carry substantial implications for regulators, hospitals, and device manufacturers broadly today. Legislators should consider establishing specific statutory frameworks dividing cybersecurity responsibility explicitly. Regulators would benefit from clearer standards evaluating compliance separately for manufacturers and hospitals. Hospitals would gain clearer guidance regarding necessary network security investment and configuration decisions. This clarified framework offers practical applicability across regulatory, healthcare, and manufacturing governance contexts. Manufacturers would face explicit expectations regarding device-level cybersecurity design and maintenance responsibilities. Patients would benefit from more predictable accountability structures following medical device cyber-attacks. Policymakers should prioritize this clarification given significant patient safety stakes involved. This research provides meaningful groundwork supporting future responsibility division framework development efforts. Legal reclassification directly addresses this ambiguity through clearly divided cybersecurity accountability standards (Layode et al., 2024).

C. Limited Legal Remedies for Patients Harmed by Device Cyber-Attacks

This finding exposes significant weaknesses within current patient protection legal mechanisms broadly. Patients suffering harm from compromised medical devices currently lack effective legal remedies available. Traditional medical malpractice frameworks assume clinical errors rather than cybersecurity related device failures. Product liability frameworks similarly struggle addressing harm resulting from third-party cyber-attacks specifically. This mismatch leaves patients without clear legal pathways pursuing meaningful compensation claims. Courts frequently dismiss claims, finding neither malpractice nor traditional product defect frameworks apply. This dismissal occurs despite clear evidence that cybersecurity failures caused genuine patient harm. Patients face substantial legal and financial barriers pursuing claims against manufacturers or hospitals. Litigation costs often exceed potential recovery, discouraging many legitimate claims entirely. Recent patient advocacy efforts have highlighted these systemic barriers facing cybersecurity harm victims. Some legal organizations have begun developing specialized resources supporting device cybersecurity harm claims. This gap demonstrates why comprehensive liability reform remains essential for meaningful patient protection (Nacu et al., 2025).

This remedy gap produces serious consequences affecting both individual patients and broader healthcare trust. Patients absorb significant harm without corresponding legal accountability from responsible manufacturers or hospitals. This imbalance removes meaningful incentives improving device cybersecurity and network protection practices voluntarily. Manufacturers and hospitals calculate minimal legal risk given weak existing patient remedy

frameworks. This calculation prioritizes cost reduction over genuine patient safety and security investment. Weak accountability structures ultimately normalize inadequate cybersecurity practices across the healthcare technology sector. Stronger legal remedies would create meaningful incentives prioritizing robust cybersecurity design and maintenance. Manufacturers and hospitals would then face genuine consequences for demonstrably inadequate security practices. This accountability could substantially reduce successful cyber-attacks against connected medical devices. Patients would gain realistic legal pathways pursuing legitimate claims against responsible parties. Establishing meaningful remedies remains essential for restoring patient trust in connected healthcare technology.

Specific examples demonstrate how limited remedies produce troubling accountability gaps for patients. Several patients harmed by compromised infusion pumps found minimal legal recourse available. Courts dismissed these cases citing insufficient evidence connecting cybersecurity failure directly to clinical harm. Similar dismissals occurred across cases involving compromised monitors and networked diagnostic equipment. This consistent pattern frustrated patients and legal advocates seeking meaningful device accountability standards. Some jurisdictions have explored strict liability theories specifically for networked medical device harm. These theories represent meaningful innovation though judicial adoption remains limited and inconsistent currently. Recent proposed legislation suggests growing legislative recognition that current remedies remain fundamentally inadequate. This evidence strengthens arguments supporting formal liability reform addressing this significant justice gap. Legal reform remains necessary for providing patients realistic pathways toward meaningful accountability.

This analysis acknowledges important limitations regarding patient remedy research and resulting conclusions. Measuring the full scope of unaddressed cybersecurity harm requires extensive additional empirical research. Available data regarding dismissed cases often lacks detailed information about underlying technical circumstances. This limitation complicates fully understanding patterns across different types of device cybersecurity harm. Additionally, establishing causation between a cyber-attack and specific clinical harm remains technically demanding. Medical experts and cybersecurity experts must often collaborate closely, increasing litigation complexity significantly. Furthermore, defining actionable cybersecurity harm requires careful balancing against legitimate innovation interests. Overly broad remedy expansion might inadvertently discourage beneficial medical technology development and adoption. These limitations suggest remedy expansion must proceed thoughtfully, balancing multiple competing important considerations.

Comparing remedy frameworks across different legal systems reveals interesting contradictions worth noting. Some legal systems assume existing malpractice and product liability theories adequately cover this harm. Evidence increasingly suggests these traditional theories poorly fit genuinely novel cybersecurity related injuries. Other systems have begun recognizing cybersecurity harm as a distinct compensable injury category. This divergence creates inconsistent patient protection depending on jurisdiction and applicable legal theory. Some advocates argue courts should simply extend existing doctrines through creative legal interpretation. Others argue specialized statutory frameworks remain necessary given unique cybersecurity harm characteristics. This disagreement highlights genuine uncertainty regarding the optimal legal reform pathway forward. These contradictions demonstrate why thoughtful, purpose-built reform likely outperforms incremental doctrinal stretching.

These findings carry substantial implications for legislators, courts, and patient advocacy organizations broadly. Legislators should consider creating specific statutory remedies addressing demonstrable cybersecurity related device harm. Courts would benefit from clearer guidance evaluating cybersecurity harm claims under reformed legal standards. Patients would gain meaningful legal pathways pursuing legitimate claims against manufacturers or hospitals. This improved framework offers practical applicability across legislative, judicial, and healthcare advocacy contexts. Manufacturers and hospitals would face appropriate incentives prioritizing genuine patient cybersecurity protection investments. Policymakers should prioritize this reform given documented patterns of device related cybersecurity harm. This research provides meaningful groundwork supporting future patient remedy development and legal reform efforts. Legal reclassification directly addresses this gap through proposed liability standards enabling meaningful patient recourse (Saleem et al., 2025).

D.Insufficient Regulatory Standards for Ongoing Device Cybersecurity Maintenance

This finding reveals significant gaps within current medical device regulatory approval frameworks broadly. Regulatory agencies primarily evaluate cybersecurity at initial device approval rather than throughout lifespan. Few regulations require manufacturers maintaining cybersecurity support for devices already sold to hospitals. This approval-focused model fails addressing vulnerabilities discovered after devices enter clinical use. Older devices often continue operating without adequate manufacturer cybersecurity support or updates. This gap leaves aging medical

device fleets particularly vulnerable to newly discovered threats. Regulators increasingly recognize this limitation but have moved slowly implementing meaningful reform. Some jurisdictions have proposed requiring manufacturers maintaining security support for specified minimum periods. These proposals represent meaningful progress though comprehensive adoption remains limited across regions currently. Recent cybersecurity incidents affecting older devices have intensified regulatory attention toward this gap. This evidence demonstrates why ongoing maintenance requirements deserve serious regulatory reform consideration. Establishing lifecycle cybersecurity standards remains essential for protecting patients using older medical devices (Martinez-Licona, 2026).

This regulatory gap produces meaningful consequences affecting healthcare institutions and patient safety broadly. Hospitals often continue using older devices without understanding their cybersecurity support status. This uncertainty leaves institutions unknowingly operating vulnerable equipment within critical care settings. Manufacturers face no regulatory requirement continuing security support once devices reach certain ages. This absence creates troubling incentives discontinuing support to reduce ongoing operational costs. Patients relying on older devices bear disproportionate cybersecurity risk without adequate protective regulatory oversight. Stronger lifecycle standards would require manufacturers maintaining transparency regarding device security support duration. Hospitals would then make informed procurement and replacement decisions based on security support timelines. This transparency would enable better institutional planning around device replacement and security management. Patients would ultimately benefit from healthcare institutions making more informed device security decisions. Establishing these standards remains crucial for protecting vulnerable patients using aging medical technology.

Specific examples illustrate consequences resulting from insufficient lifecycle cybersecurity regulation currently. Several hospitals continued operating imaging and monitoring equipment years after manufacturer support ended. Investigations following related incidents revealed hospitals where unaware support had actually ceased. This lack of awareness stemmed partly from unclear manufacturer communication regarding support timelines. Some manufacturers quietly discontinued patches without formally notifying hospital customers of the change. Regulators in several jurisdictions have proposed mandatory end-of-support notification requirements addressing this gap. These proposals represent meaningful progress though implementation remains inconsistent across different regulatory regions. Recent legislative hearings have highlighted aging device fleets as a significant patient safety concern. This evidence demonstrates why lifecycle cybersecurity regulation deserves urgent legislative and regulatory attention.

This analysis acknowledges important limitations regarding lifecycle cybersecurity regulation research and design. Determining an appropriate minimum support period requires balancing patient safety against manufacturer feasibility. Devices vary significantly in complexity, cost, and expected clinical lifespan across different categories. This variation complicates establishing a single, universally applicable minimum support period standard. Additionally, rapidly evolving cybersecurity threats may require support extending well beyond initial expectations. Manufacturers may struggle predicting long-term support costs when initially pricing and designing devices. Furthermore, some hospitals may resist replacing functional equipment despite lapsed cybersecurity support status. This resistance reflects genuine budget constraints rather than disregard for patient safety concerns. These limitations suggest lifecycle standards must remain flexible while still providing meaningful minimum protections.

Comparing regulatory approaches across jurisdictions reveals interesting contradictions worth examining thoughtfully. Some regulators assume market pressure alone will encourage manufacturers extending cybersecurity support voluntarily. Evidence suggests manufacturers often prioritize new product development over supporting existing device fleets. Other regulators have moved toward mandatory minimum support periods enforced through regulatory approval processes. This divergence creates inconsistent patient protection depending on manufacturer location and target market. Some industry representatives argue mandatory support periods might discourage innovation and increase device costs. Patient advocates counter that safety should not depend on voluntary corporate goodwill alone. This disagreement reflects a genuine tension between innovation incentives and baseline patient protection needs. These contradictions demonstrate why carefully calibrated mandatory minimums likely outperform purely voluntary approaches.

These findings carry substantial implications for regulators, manufacturers, and healthcare procurement decision-makers broadly. Regulators should consider establishing mandatory minimum cybersecurity support periods for medical devices. Manufacturers would benefit from clearer expectations guiding long-term cybersecurity investment planning decisions. Hospitals would gain valuable information supporting more informed device procurement and replacement decisions. This improved framework offers practical applicability across regulatory, manufacturing, and healthcare procurement contexts. Patients would benefit from reduced cybersecurity risk resulting from better-managed device replacement cycles. Policymakers should prioritize this reform given aging medical device

fleets across many hospitals. This research provides meaningful groundwork supporting future lifecycle cybersecurity regulation development efforts. Legal reclassification combined with lifecycle standards addresses this gap through sustained manufacturer accountability requirements (Evershine et al., 2024).

E.Supply Chain Complexity Complicating Cybersecurity Liability Determination

This finding reveals significant challenges arising from complex medical device supply chain structures. Medical devices often incorporate software, chips, and components from numerous different suppliers globally. This complexity complicates determining which specific party caused a particular cybersecurity vulnerability. Courts struggle allocating liability when vulnerabilities originate from third-party components rather than manufacturers. Device manufacturers sometimes lack complete visibility into security practices of their own suppliers. This limited visibility complicates manufacturers' ability preventing vulnerabilities embedded within purchased components. Legal frameworks provide little guidance addressing liability across these complex multi-party relationships. Some scholars have proposed requiring manufacturers maintaining comprehensive supply chain security verification processes. These proposals represent meaningful progress though practical implementation remains genuinely challenging currently. Recent high-profile supply chain attacks have intensified attention toward this complex vulnerability. This evidence demonstrates why supply chain accountability deserves serious legal and regulatory consideration. Establishing clearer supply chain liability standards remains essential for comprehensive device cybersecurity accountability (Qazi, 2025).

This supply chain complexity produces meaningful consequences affecting accountability throughout the medical device industry. Component suppliers face minimal direct legal accountability despite contributing vulnerabilities into medical devices. Device manufacturers bear primary legal exposure despite limited control over third-party component security. This mismatch between control and liability creates troubling accountability gaps throughout the supply chain. Patients ultimately bear consequences regardless of which specific supply chain party caused vulnerabilities. Clearer supply chain liability standards would better align legal responsibility with actual security control. Component suppliers would then face appropriate incentives maintaining robust security practices themselves. Manufacturers would gain clearer standards for evaluating and selecting security-conscious component suppliers. This alignment would strengthen overall device security throughout the entire manufacturing supply chain. Patients would benefit from improved security resulting from accountability throughout the supply chain. Achieving this alignment requires careful legal framework design addressing complex multi-party relationships.

Specific examples illustrate consequences resulting from unresolved supply chain cybersecurity liability gaps. Several device recalls resulted from vulnerabilities traced to a single shared software component. This component appeared across products from multiple different manufacturers simultaneously affected by the flaw. Determining appropriate liability proved difficult given the component supplier's limited direct relationship with patients. Some manufacturers absorbed remediation costs entirely despite the vulnerability originating outside their direct control. Other manufacturers pursued lengthy contractual disputes with suppliers regarding cost and responsibility allocation. These disputes often outlasted the immediate patient safety concern requiring urgent remediation. Some industry consortiums have proposed shared security certification standards for common device components. These certification efforts represent promising progress though widespread adoption remains still developing. This evidence demonstrates why supply chain liability clarity remains urgently needed industry-wide.

This analysis acknowledges important limitations regarding supply chain liability research and framework design. Defining appropriate supplier obligations requires balancing practical feasibility against meaningful accountability standards. Global supply chains often span multiple countries with differing legal traditions and enforcement capacity. This variation complicates creating universally applicable supply chain liability standards across jurisdictions. Additionally, component suppliers often serve numerous industries beyond healthcare, complicating tailored regulatory approaches. Requirements designed specifically for medical device supply chains may not translate cleanly elsewhere. Furthermore, rapidly evolving component technology complicates maintaining current and relevant security verification standards. These limitations suggest supply chain liability frameworks must remain adaptable and internationally coordinated. Achieving meaningful reform requires sustained collaboration between regulators, manufacturers, and component suppliers.

Comparing supply chain accountability approaches reveals interesting contradictions worth examining carefully. Some manufacturers assume contractual indemnification clauses with suppliers adequately manage cybersecurity risk exposure. Evidence suggests these contractual protections often prove difficult enforcing amid urgent patient safety concerns. Other manufacturers have begun requiring independent security audits of suppliers before component integration. This proactive approach represents meaningful progress though it remains

inconsistently adopted industry-wide. Some regulators favor holding manufacturers fully accountable regardless of supply chain complexity involved. Others favor distributing accountability proportionally across the supply chain based on demonstrated contribution. This disagreement reflects genuine difficulty allocating liability fairly across complex manufacturing relationships. These contradictions demonstrate why thoughtful, multi-party frameworks likely outperform simplistic single-party liability models.

These findings carry substantial implications for manufacturers, component suppliers, and regulatory policymakers broadly. Regulators should consider requiring manufacturers maintaining documented supply chain security verification processes. Component suppliers would face appropriate incentives improving their own cybersecurity practices and standards. Manufacturers would benefit from clearer standards supporting informed component supplier selection decisions. This improved framework offers practical applicability across regulatory, manufacturing, and supply chain governance contexts. Patients would benefit from strengthened security throughout the entire medical device supply chain. Policymakers should prioritize this reform given increasing complexity of modern medical device manufacturing. This research provides meaningful groundwork supporting future supply chain liability framework development efforts. Legal reclassification combined with supply chain standards addresses this gap through comprehensive accountability mechanisms (Nwani et al., 2025).

F.Weak Enforcement Mechanisms for Medical Device Cybersecurity Compliance

This finding reveals significant weaknesses within current medical device cybersecurity enforcement mechanisms broadly. Regulators possess limited authority compelling manufacturers maintaining adequate ongoing cybersecurity practices consistently. This weak enforcement allows manufacturers deprioritizing cybersecurity investment without facing meaningful regulatory consequences. Companies calculate minimal enforcement risk, reducing incentives prioritizing robust cybersecurity design and maintenance. Some regulatory agencies lack sufficient technical expertise evaluating manufacturer cybersecurity compliance claims accurately. This expertise gap complicates meaningful enforcement even where regulatory authority technically exists. Recent policy discussions have emphasized needing stronger enforcement mechanisms alongside cybersecurity standards themselves. Some jurisdictions have proposed increasing regulatory funding supporting dedicated medical device cybersecurity enforcement units. These proposals represent meaningful progress though implementation across jurisdictions remains still limited. Recent cybersecurity incidents have intensified public and regulatory attention toward enforcement weaknesses. This evidence demonstrates why strengthened enforcement deserves serious policy and legislative consideration. Establishing robust enforcement mechanisms remains essential for translating cybersecurity standards into genuine compliance (Ludvigsen, 2023).

This enforcement gap produces meaningful consequences affecting genuine cybersecurity compliance across the medical device industry. Manufacturers facing weak enforcement may treat cybersecurity standards as merely aspirational guidelines. This treatment undermines the practical effectiveness of otherwise well-designed cybersecurity regulatory frameworks. Patients bear consequences when manufacturers' actual practices fail matching stated regulatory compliance claims. Strengthened enforcement would create meaningful consequences for manufacturers failing genuine cybersecurity compliance obligations. Manufacturers would then face real incentives investing in verifiable, robust cybersecurity practices consistently. This accountability could substantially improve actual device security beyond mere paper compliance. Patients would benefit from manufacturers treating cybersecurity as a genuine operational priority. Establishing meaningful enforcement remains fundamental for translating cybersecurity regulations into genuine patient protection. This translation from policy to practice depends entirely on credible regulatory enforcement mechanisms.

Specific examples illustrate consequences resulting from weak medical device cybersecurity enforcement currently. Several manufacturers faced regulatory warnings for cybersecurity shortcomings without subsequent meaningful penalty enforcement. These warnings often lacked deadlines or verification mechanisms confirming manufacturers addressed identified concerns. Some manufacturers continued selling affected devices despite unresolved warnings remaining formally outstanding. Regulators publicly acknowledged these enforcement gaps but cited limited resources preventing stronger action. Some jurisdictions have since increased funding for dedicated medical device cybersecurity enforcement teams. These increases represent meaningful progress though comparable investment remains uneven across different regions. Recent legislative proposals suggest growing recognition that enforcement capacity requires substantial ongoing investment. This evidence demonstrates why strengthened enforcement capacity deserves sustained legislative and budgetary attention.

This analysis acknowledges important limitations regarding cybersecurity enforcement research and policy recommendations. Measuring actual enforcement effectiveness requires access to detailed regulatory compliance and investigation data. This data often remains confidential or incomplete, limiting comprehensive external research access. Additionally, appropriate enforcement intensity may vary depending on device risk category and complexity. High-risk implanted devices likely warrant different enforcement priorities than lower-risk monitoring equipment. Furthermore, enforcement capacity depends heavily on political will and available government budgetary resources. These factors vary considerably across different countries and political administrations over time. These limitations suggest enforcement reform must remain adaptable to changing resource and political circumstances. Sustained institutional commitment remains necessary regardless of short-term political or budgetary fluctuations.

Comparing enforcement approaches across different regulatory systems reveals interesting contradictions worth noting. Some regulators favor cooperative, guidance-based approaches encouraging voluntary manufacturer cybersecurity improvement. Evidence suggests voluntary approaches often produce inconsistent and insufficient improvement absent genuine enforcement pressure. Other regulators favor stricter, penalty-based enforcement approaches with meaningful financial consequences. This divergence reflects differing philosophies regarding effective methods achieving genuine regulatory compliance. Some industry representatives argue punitive enforcement might discourage manufacturers from voluntary vulnerability disclosure. Patient advocates counter that weak enforcement ultimately incentivizes concealment rather than proactive disclosure. This disagreement highlights genuine tension between encouraging transparency and ensuring meaningful accountability. These contradictions demonstrate why carefully calibrated enforcement approaches likely outperform purely cooperative models.

These findings carry substantial implications for regulators and medical device policy enforcement authorities broadly. Regulators should consider increasing enforcement resources and technical expertise supporting cybersecurity compliance verification. Legislators would benefit from granting regulators stronger authority compelling manufacturer cybersecurity accountability. Manufacturers would face appropriate incentives prioritizing genuine cybersecurity investment given credible enforcement mechanisms. This improved framework offers practical applicability across regulatory, legislative, and manufacturing governance contexts. Patients would benefit from improved device security resulting from meaningful regulatory enforcement mechanisms. Policymakers should prioritize this strengthening given documented patterns of inadequate cybersecurity compliance. This research provides meaningful groundwork supporting future enforcement mechanism development and implementation efforts. Legal reclassification combined with strengthened enforcement addresses this gap through credible accountability mechanisms (Djeffal et al., 2025).

H. Implication

This research challenges traditional product liability theories assuming defects exist only at initial sale. Classical liability frameworks focus on manufacturing quality rather than ongoing cybersecurity maintenance needs. These findings suggest cybersecurity maintenance deserves formal recognition as a continuing manufacturer duty. This shift would strengthen accountability while creating new ongoing compliance obligations for manufacturers. Positive outcomes include stronger patient protection, clearer liability standards, and improved healthcare cybersecurity governance. Negative consequences might include increased manufacturer costs and potential pricing impacts on medical devices. Regulators could use these findings designing lifecycle cybersecurity frameworks addressing device support duration. Current legal frameworks remain outdated, fragmented, and poorly suited addressing networked medical technology risks. Real-world application requires courts recognizing ongoing cybersecurity maintenance within existing liability frameworks meaningfully. Policymakers might introduce mandatory support period requirements alongside clearer manufacturer-hospital responsibility division standards. Manufacturers, hospitals, patients, and regulators would all benefit from this clarified accountability framework. Recent initiatives, including proposed medical device cybersecurity legislation, reflect growing momentum toward reform.

CONCLUSION

Connected medical devices increasingly expose patients to significant cybersecurity related safety risks. This research examined how legal liability should apply following medical device cyber-attacks. Treating devices under outdated liability frameworks ignores genuine ongoing cybersecurity maintenance needs. Current legal frameworks lack clear criteria dividing responsibility between manufacturers and healthcare institutions. Patients similarly lack effective remedies challenging parties for cybersecurity related device harm. Regulatory gaps across jurisdictions further complicate achieving consistent device cybersecurity accountability standards. These interconnected gaps

demonstrate why liability reform deserves serious legal and policy attention. Recent regulatory initiatives, including proposed device cybersecurity legislation, reflect growing awareness of these gaps. However, meaningful legal reform remains slow, fragmented, and inconsistent across different jurisdictions globally. This research connects cybersecurity practices, legal theory, and patient safety within one coherent framework. Connected medical devices continue growing more prevalent, making this legal gap increasingly urgent.

Three central arguments emerged throughout this research supporting formal liability reform efforts. First, courts lack clear standards addressing ongoing cybersecurity maintenance as a manufacturer duty. Second, responsibility division between manufacturers and hospitals remains genuinely unclear under current frameworks. Third, weak enforcement mechanisms prevent cybersecurity standards from achieving meaningful real-world compliance. These arguments collectively demonstrate systemic weaknesses spanning multiple interconnected regulatory and legal areas. Addressing one gap alone would prove insufficient without comprehensive coordinated reform efforts. Liability reform offers a unifying framework connecting these previously fragmented regulatory and legal concerns. This approach strengthens accountability while providing clearer guidance for manufacturers and healthcare institutions. Stronger frameworks would benefit patients, hospitals, manufacturers, and broader healthcare cybersecurity governance. This research demonstrates why isolated legal reforms cannot adequately address modern medical device risks. A comprehensive approach remains essential for achieving genuine medical device accountability improvements.

These findings carry meaningful implications extending beyond academic legal scholarship into practical healthcare policy. Policymakers could use this research designing lifecycle cybersecurity and responsibility division standards. Courts could apply proposed criteria evaluating manufacturer and hospital cybersecurity accountability appropriately. Regulators might introduce mandatory support timelines alongside strengthened enforcement mechanisms for compliance. Healthcare institutions could develop procurement policies informed by these proposed accountability frameworks. Future research should examine how specific liability reform proposals perform across jurisdictions. Researchers might also study emerging technologies affecting evolving medical device cybersecurity questions. Additional studies could explore implementation challenges facing smaller healthcare institutions specifically under reform. This research provides a foundation supporting continued scholarly and policy development efforts. Addressing these gaps remains essential for building genuinely accountable connected healthcare technology systems.

BIBLIOGRAPHY

Aldosari, B. (2025). Cybersecurity in healthcare: New threat to patient safety. *Cureus, 17*(5), e83614. https://doi.org/10.7759/cureus.83614

AllahRakha, N. (2025). Sustainable ICT infrastructure and green technologies in the Caribbean. *Industrial Engineering and Management Journal, 3*(1), 4–12. https://doi.org/10.47412/CLVD2784

AllahRakha, N. (2026). Legal analysis of the law of the Republic of Uzbekistan "On Payments and Payment System". *TSUL Legal Report,* 5(1), 38–55. https://doi.org/10.51788/tsul.lr.5.1./WAJR6426

Conceição, F., Rocha, M., & Almeida, F. (2026). Security compliance as a catalyst for sustainable partnerships: A design science approach for SMEs. *Journal of Cybersecurity and Privacy, 6*(2), 53. https://doi.org/10.3390/jcp6020053

Djeffal, C. (2025). *Law by design obligations: The future of regulating digital technologies in Europe? Computer Law & Security Review, 59*, Article 106232. https://doi.org/10.1016/j.clsr.2025.106232

Evershine CPAs Firm. (2024). *Taiwan medical devices registration*. Evershine CPAs Firm. https://www.evershinecpa.com/

Freyer, O., Jahed, F., Ostermann, M., Rosenzweig, C., Werner, P., & Gilbert, S. (2024). Consideration of cybersecurity risks in the benefit-risk analysis of medical devices: Scoping review. *Journal of Medical Internet Research, 26*, e65528. https://doi.org/10.2196/65528

Gennari, F. (2025). (Product) liability in the Medical Internet of Things. What now? In F. Casarosa, F. Gennari, & A. Rossi (Eds.), *Enabling and safeguarding personalized medicine* (pp. 317–338). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-99709-9_16

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications, 1*, 100016. https://doi.org/10.1016/j.csa.2023.100016

Jubaidi, D., & Khoirunnisa, K. (2025). *Legal perspectives on the risks of medical malpractice in the implementation of artificial intelligence and telemedicine technologies. ALADALAH: Jurnal Politik Sosial Hukum dan Humaniora, 3*(4), 77–100. https://doi.org/10.59246/aladalah.v3i4.1647

Layode, O., Naiho, H. N. N., Adeleke, G. S., Udeh, E. O., & Labake, T. T. (2024). *The role of cybersecurity in facilitating sustainable healthcare solutions: Overcoming challenges to protect sensitive data. International Medical Science Research Journal, 4*(6), 668–693. https://doi.org/10.51594/imsrj.v4i6.1228

Ludvigsen, K. R. (2023). The role of cybersecurity in medical devices regulation: Future considerations and solutions. *Law, Technology and Humans, 5*(2), 59–77. https://doi.org/10.5204/lthj.3080

Ludvigsen, K. R. (2023). The role of cybersecurity in medical devices regulation: Future considerations and solutions. *Law, Technology and Humans, 5*(2), 59–77. https://doi.org/10.5204/lthj.3080

Ludvigsen, K. R. (2023). *The role of cybersecurity in medical devices regulation: Future considerations and solutions. Law, Technology and Humans, 5*(2), 59–77. https://doi.org/10.5204/lthj.3080

Martinez-Licona, F. M. (2026). AI in medical devices: Regulatory challenges and the path forward. *Health and Technology, 16*, 659–669. https://doi.org/10.1007/s12553-026-01077-8

McDermott, O., Foley, I., Antony, J., Sony, M., & Butler, M. (2022). The impact of Industry 4.0 on the medical device regulatory product life cycle compliance. *Sustainability, 14*(21), 14650. https://doi.org/10.3390/su142114650

Menon, V. (2026). Cybersecurity breaches in medical devices: Analyzing FDA safety communications in response to patient security concerns. *Frontiers in Digital Health, 8*, 1701551. https://doi.org/10.3389/fdgth.2026.1701551

Nacu, A. G., Constantin, D. A., & Rogozea, L. M. (2025). Ethical dilemmas and legal responsibilities in patient care: An analysis of hospital safety. *Healthcare, 13*(21), 2800. https://doi.org/10.3390/healthcare13212800

Nwani, S. (2025). *Evaluating the impact of blockchain technology on supply chain transparency and traceability. Gulf Journal of Advance Business Research, 3*(6), 1065–1093. https://doi.org/10.51594/gjabr.v3i6.149

Ostermann, M., Mathias, R., Jahed, F., Parker, M. B., Hudson, F. D., Harding, W. C., Gilbert, S., & Freyer, O. (2025). Cybersecurity requirements for medical devices in the EU and US: A comparison and gap analysis of the MDCG 2019-16 and FDA premarket cybersecurity guidance. *Computational and Structural Biotechnology Journal, 28*, 259–266. https://doi.org/10.1016/j.csbj.2025.07.024

Petrov, I., & Kumar, R. (2025). *Disinformation and legal responsibility: Regulating digital speech without curtailing dissent. Interdisciplinary Studies in Society, Law, and Politics, 4*(2), 303–314. https://doi.org/10.61838/kman.isslp.4.2.26

Qazi, A. (2025). Systemically important supply chains in crisis: Mapping disruptions and global ripple effects. *Natural Hazards Research*. Advance online publication. https://doi.org/10.1016/j.nhres.2025.09.003

Saleem, H. A. R., Bukhtiar, A., Zaheer, B., & Farooq, M. A. U. (2025). *Challenges faced by the judiciary in implementing cybersecurity laws in Pakistan. The Critical Review of Social Sciences Studies, 3*(1), 1052–1066. https://doi.org/10.59075/1wyx0v30

Schorr, M. (2024). *How will the new Product Liability Directive (EU) 2024/2853 impact businesses?* Keystone Law. https://www.keystonelaw.com/

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. *Medical Devices: Evidence and Research, 8*, 305–316. https://doi.org/10.2147/MDER.S50048