ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Enhancing Network Security in Healthcare Institutions: Addressing Connectivity and Data Protection Challenges

Srikanth Bellamkonda

Danta Technologies Inc, Colorado, USA

ABSTRACT: The rapid adoption of digital technologies in healthcare has revolutionized patient care, enabling seamless data sharing, remote consultations, and enhanced medical record management. However, this digital transformation has also introduced significant challenges to network security and data protection. Healthcare institutions face a dual challenge: ensuring uninterrupted connectivity for critical operations and safeguarding sensitive patient information from cyber threats. These challenges are exacerbated by the increased use of interconnected devices, electronic health records (EHRs), and cloud-based solutions, which, while enhancing efficiency, expand the attack surface for malicious actors. This research focuses on addressing the pressing need for robust network security in healthcare institutions. It examines the unique vulnerabilities of healthcare networks, including the risks posed by outdated infrastructure, insufficient encryption protocols, and the lack of standardized security practices across systems. The paper highlights the critical role of advanced cybersecurity frameworks, such as zero-trust architectures and real-time threat detection systems, in mitigating risks. Additionally, it explores the integration of artificial intelligence (AI) and machine learning (ML) in enhancing the predictive capabilities of security tools, enabling institutions to proactively identify and neutralize potential threats. Connectivity remains a cornerstone of modern healthcare operations, facilitating collaboration among healthcare providers and ensuring timely access to patient data. However, maintaining connectivity without compromising security is a complex task. This research delves into strategies for achieving this balance, such as implementing secure Virtual Private Networks (VPNs), multi-factor authentication (MFA), and end-to-end encryption. It also emphasizes the importance of regular network assessments, employee training programs, and the adoption of compliance standards like HIPAA to ensure a secure and resilient network environment. The study includes case analyses of healthcare institutions that successfully navigated cybersecurity challenges, providing actionable insights into effective practices and lessons learned. These examples underscore the importance of integrating technological solutions with a culture of security awareness, emphasizing collaboration between IT professionals and medical staff. As cyber threats continue to evolve, healthcare institutions must remain vigilant and adaptive, embracing innovative solutions to safeguard their networks and protect patient data. This paper contributes to the broader discourse on cybersecurity in healthcare by proposing a comprehensive approach that addresses connectivity and data protection challenges while fostering operational efficiency. By prioritizing network security, healthcare institutions can build trust with patients, comply with regulatory requirements, and ensure the uninterrupted delivery of quality care. This research provides a roadmap for healthcare organizations seeking to strengthen their cybersecurity posture, highlighting the necessity of adopting a proactive, multi-layered approach to combat emerging threats. It calls for continuous investment in advanced technologies and emphasizes the role of collaboration among stakeholders to create a secure and connected healthcare ecosystem.

KEYWORDS: Healthcare Network Security Solutions; Data Protection in Medical Systems; Connectivity Challenges in Healthcare IT; Cybersecurity in Patient Data Management; Advanced Security Strategies for Healthcare Networks

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

I. INTRODUCTION

Healthcare institutions suffered more than 700 major data breaches in 2019. These breaches exposed millions of patient records and cost the industry billions of dollars. Digital transformation in healthcare has improved patient care but created new cybersecurity challenges. Healthcare institutions now deal with connected medical devices and electronic health records. Each digital touchpoint becomes a potential target that cybercriminals can exploit. Patient information needs protection, and healthcare operations must remain secure.

This piece outlines key strategies to protect healthcare networks. You'll learn about current threats and regulatory requirements that affect patient data protection. The discussion covers strong access controls, IoT medical device security, HIPAA compliance, and encrypted communication channels.

II. UNDERSTANDING HEALTHCARE NETWORK SECURITY LANDSCAPE

Cybersecurity threats targeting healthcare institutions have reached alarming levels. Healthcare now ranks among the top 10 targeted industries in the last four quarters. These escalating threats need an immediate and strategic response.

Current Threat Environment

The digital world of cyber threats has changed healthcare security dramatically. Organizations lose an average of USD 8,64,570.55 each day when cyber incidents cause downtime. Several dangerous threats now target healthcare systems:

- Ransomware attacks targeting critical infrastructure
- Data breaches compromising patient records
- Medical device vulnerabilities
- Distributed denial-of-service (DDoS) attacks
- Supply chain compromises

These attacks mean more than just money lost - they put patient care and safety at risk. Recent ransomware attacks have forced hospitals to turn away patients and blocked access to vital medical records.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Regulatory Requirements

The Security Rule sets national standards to protect electronic health information. Healthcare providers must put in place three essential safeguards:

Safeguard Type Key Requirements Administrative Risk analysis, security management processes Physical Facility access controls, device security Technical Access control, encryption, audit controls Healthcare organizations should maintain appropriate safeguards while ensuring electronic Protected Health Information's (ePHI) confidentiality, integrity, and availability.

Risk Assessment Framework

Risk assessment works as an ongoing process with several vital components. Healthcare organizations must conduct detailed risk analysis under Administrative Safeguards provisions. This involves:

1. Reviewing potential risks to ePHI
2. Implementing appropriate security measures
3. Documenting chosen security measures
4. Maintaining continuous security protections

A thorough risk assessment identifies and analyzes potential ePHI risks. Organizations then implement security measures to reduce vulnerabilities to acceptable levels. The Department of Health and Human Services (HHS) knows healthcare organizations vary from small providers to large multi-state health plans. This makes the framework adaptable to different organizational needs.

The Security Rule's requirements enhance privacy protections while promoting two additional vital goals: data integrity prevents unauthorized changes and ensures authorized users can access information. Regular monitoring and periodic reviews help track ePHI access, detect security incidents, and review emerging risks.

III. NETWORK ARCHITECTURE BEST PRACTICES

Healthcare networks need a strong architecture that comes from careful planning and smart implementation. Patient data protection requires multiple security layers to handle both existing and future threats.

Segmentation Strategies

Network segmentation serves as our primary defense to limit attack surfaces and reduce risks. We arrange the network into separate zones based on how sensitive the data is and what each section needs to do. This segmentation strategy works best when we combine it with other security measures to provide the highest level of protection.

Network Zone Primary Purpose Security Level Clinical Patient Care Highest Administrative Operations High Guest Public Access Standard Separating critical systems helps healthcare organizations limit damage from potential attacks and makes regulatory compliance easier.

Access Control Implementation

Our security approach creates secure authentication paths without sacrificing efficiency. These critical components make up our strategy:

- Network access control (NAC) protects applications and data at a granular level
- Identity-based security ensures that only authorized users can access specific applications
- Multi-factor authentication systems provide extra protection

These controls help us maintain 99.999% network availability while moving data smoothly between clinical devices and caregivers.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Traffic Monitoring Systems

Our traffic monitoring keeps the network healthy and secure. The systems show up-to-the-minute data about network access activities. This helps us:

1. Keep watch over operational conditions
2. Solve access issues with context-aware guidance
3. Create standard reports for trend analysis
4. Keep track of network performance

We detect unusual patterns and respond to security threats before they affect patient care through constant monitoring and active threat hunting. Our policy-based automated enforcement of network segmentation stops unauthorized activities before they start.

Clinical environments require a balance between security and patient care needs. Unknown devices automatically go to a guest network, but patient care devices need a "Human Intelligence over Artificial Intelligence" approach. Security and biomedical teams prefer human oversight instead of full automation.

Securing Medical IoT Devices

Medical device security has become a pressing concern as cybersecurity threats keep evolving and targeting healthcare institutions. Recent studies show that cyberattacks hit over 90% of healthcare units using IoT. Healthcare institutions need strong security measures to protect these vital systems.

Device Authentication Protocols

Multi-layered authentication mechanisms help secure medical devices. The goal is to ensure that only authorized parties can access medical device data and systems. The authentication framework has:

- Strong password policies
- Multi-factor authentication
- Digital signatures for firmware verification
- Secure boot mechanisms
- Access control policies

Firmware Security Management

The firmware security strategy tackles the growing complexity of medical device ecosystems. Security updates need up to 3 months for a full assessment and implementation. A structured approach to firmware management helps address these challenges.

Security Aspect Implementation Strategy Update Management Over-the-air firmware updates Validation Manufacturer verification Monitoring Real-time status tracking Recovery Secure rollback mechanisms Firmware updates fix bugs and patch security issues. They play a vital role in keeping devices safe and working effectively. The management process tracks any signs of security breaches or operational issues continuously.

IV. NETWORK ISOLATION TECHNIQUES

Network isolation serves as a key defense mechanism for medical devices. Separate network segments create extra security layers that restrict the scope and effects of potential breaches.

The FDA highlights several security objectives that shape the isolation strategy:

- Authenticity and integrity verification
- Proper authorization controls
- System availability maintenance
- Data confidentiality protection
- Timely update capabilities

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

The network isolation plan addresses unique medical device challenges. These devices often last more than 10 years, and hospital IT departments face restrictions on device updates. Granular permission levels and detailed device security logs provide strong protection for the medical device ecosystem.
The security framework actively monitors device behavior and controls network traffic to block unauthorized access. This detailed approach optimizes device security and operational efficiency while meeting regulatory requirements.

Data Protection Strategies
Healthcare data protection needs both strong technical controls and operational procedures. We created complete strategies that line up with regulatory requirements and industry best practices.

Encryption Standards
Our encryption framework follows the National Institute of Standards and Technology (NIST) guidelines to maximize data protection. AES encryption with a minimum key size of 128 bits protects all health information. Security improves with advanced solutions that support 192-bit and 256-bit encryption.
Data State Encryption Standard Implementation At Rest NIST SP 800-111 Full disk encryption In Transit NIST SP 800-52 TLS protocols Mobile Devices AES-256 Device-level encryption Backup Solutions

Our multi-tiered backup strategy combines local and cloud storage solutions to guarantee data availability. Experience shows that backups need frequent updates to multiple locations, with mandatory encryption and regular testing.
Our backup strategy's core elements are:

- Encrypted data storage in transit and at rest
- Multiple backup copies across different locations
- Regular backup verification and testing
- Flexible recovery options for files and systems
- Automated monitoring of backup success rates

Hybrid backup solutions give us the best balance of security and accessibility. This method pairs on-site backups for quick access with off-site storage more than 150 miles away from the facility for disaster recovery.

Data Loss Prevention
Our data loss prevention (DLP) strategy protects structured and unstructured healthcare data. Healthcare data remains unstructured nearly 80% of the time, so we use complete monitoring systems to track and secure various data formats.
Real-time monitoring and proactive controls help us watch our entire data landscape. Our DLP system sends automated alerts for suspicious activities and unauthorized access attempts. Role-based access controls ensure staff members can only see patient records needed for their job duties.
Our DLP solutions work with threat intelligence systems to improve protection. This connection helps us spot and block potential data leaks before they happen. Security assessments and DLP policy updates happen regularly to tackle new threats and vulnerabilities.
This all-encompassing approach to data protection maintains HIPAA compliance and operational efficiency. Security measure testing, automated monitoring, and employee training help us stay ahead of emerging threats while keeping critical healthcare data accessible.

V. CLOUD INTEGRATION SECURITY

Healthcare environments need a strategic approach to security when integrating cloud services. Hybrid cloud computing has become crucial for healthcare organizations. It provides both security control and operational flexibility.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Hybrid Cloud Architecture
Healthcare organizations can handle fluctuating demands while keeping strict security protocols through hybrid cloud architecture. This architecture combines the strengths of private and public cloud environments. Our hybrid cloud framework has:

Component Primary Function Security Benefit Private Cloud Critical Data Storage Enhanced Control Public Cloud Operational Workflows Cost Efficiency On-premises Systems Immediate Access Direct Oversight Healthcare teams can transfer data securely between different platforms through this architecture. This improves collaboration and maintains data integrity.

Data Migration Security
Multiple layers of protection safeguard data migration. Healthcare organizations face unique challenges during migration. Data breaches cost an average of USD 8,64,570.55 per day in downtime. The system addresses these risks through:

- End-to-end encryption for data in transit
- Automated validation of transferred data
- Incremental data transfer protocols
- Immediate synchronization monitoring
- Complete backup systems

AWS DataSync automates many transfer processes efficiently. This ensures data consistency and reduces migration time. The system maintains data availability during peak demand periods while meeting security standards.

Cloud Access Controls
Access control mechanisms line up with HIPAA requirements and industry best practices. Identity and Access Management (IAM) follows strict least-privilege principles. The system authenticates user identities through:

1. Multi-factor authentication protocols
2. IP-based access restrictions
3. Time-based access controls
4. Custom policy attachments

AWS Key Management Service (KMS) works with CloudTrail to log all encryption key access instances. This monitoring system tracks and audits all data access attempts. Healthcare regulations compliance remains assured.
AWS Trusted Advisor monitors the infrastructure for potential vulnerabilities and ways to optimize. This helps identify and address security concerns before they affect patient care or data integrity.

The cloud security measures create a reliable framework that supports operational efficiency and regulatory compliance. Healthcare organizations get the flexibility they need through hybrid cloud architecture. Patient information stays protected with stringent security controls.

Real-time Monitoring and Response
Live monitoring and incident response are the foundation of our healthcare cybersecurity strategy. Our team has set up detailed monitoring tools that track data and process events as they happen. These tools turn information into useful metrics and key performance indicators.

VI. SECURITY INFORMATION MANAGEMENT

A strong security information management system gives us live visibility throughout our healthcare network. The system has customizable information dashboards showing critical metrics and performance indicators. Key features include:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

- Automated notification mechanisms on multiple platforms
- Customized KPI tracking and metrics
- Visual interface for process monitoring
- Live event correlation and analysis

Our monitoring infrastructure adds an extra protection layer. This helps reduce mortality rates and length of stay while avoiding increased costs from treating complications.

Incident Response Protocols

The NIST-recommended lifecycle guides our incident response framework to handle security events systematically. Phase Key Activities Preparation Documentation and planning Detection Threat identification and analysis Containment Preventing the spread of incidents Recovery System restoration and verification Research shows 77% of organizations fail to consistently apply formal incident response plans. Our team created a structured approach with detailed documentation of all incident-related actions to address this issue. Response protocols focus on:

1. Swift containment strategies to prevent threat propagation
2. Detailed analysis of breach vectors
3. Systematic recovery procedures
4. Detailed post-incident review

Threat Intelligence Integration

Cyber threat intelligence (CTI) integration has strengthened our security stance. Microsoft collects 65 trillion security signals daily from the global threat landscape. Our threat intelligence platform delivers:

- Automated enrichment of threat data
- Healthcare-specific dashboard configurations
- Pre-built connectors for specialized threat feeds
- Live threat correlation and analysis

Automation works with CTI to find weaknesses in our defenses and uncover likely attack vectors. This method works especially well against ransomware-as-a-service (RaaS) attacks that often exploit poor cyber hygiene and weak authentication controls.

Our proactive defense against emerging threats relies on continuous monitoring and threat intelligence integration. The system has automated escalation procedures based on specific criteria. Critical alerts reach the right personnel through multiple channels including email, pager, and SMS notifications.

Compliance and Audit Management

Our healthcare security framework relies on effective compliance and audit management systems as its lifeblood. We've created an integrated system that makes compliance activities smoother. This reduces administrative work and leads to substantial cost savings while making patient care safer.

HIPAA Requirements

A detailed security management process helps us stay compliant with HIPAA Security Rule requirements. We focus on three main areas:

Safeguard Type Key Components Implementation Focus Administrative Risk Analysis Security Management Physical Access Controls Facility Security Technical Encryption Data Protection Regular reviews and updates keep our security measures effective at protecting electronic protected health information (ePHI). Our experience shows that bringing compliance programs together helps solve conflicts between different standards and cuts down on administrative work.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Documentation Procedures

Our documentation procedures line up with HIPAA requirements. The system keeps all security-related documents for six years from when they were created or last used. Our documentation strategy includes:

- Written security policies and procedures
- Records of required actions and assessments
- Regular reviews and updates based on environmental changes
- Detailed incident response documentation
- Training and awareness program records

We've cut down on duplicate documentation by bringing healthcare compliance management together. This makes compliance processes more efficient and reduces work across departments.

Audit Trail Implementation

Our reliable audit trail system tracks all ePHI interactions in detail. The audit logs keep essential information about data access and changes for at least six years. We watch:

1. User access and authentication attempts
2. Changes to system configurations
3. Data modifications and transfers
4. Security incident responses

The audit trail system works especially well when detecting and stopping unauthorized access, and it sends automatic alerts for suspicious activities. We assess risks regularly to spot potential weak points and guide our security measures. Detailed audit trails help us prove we're taking proper care of patient information. Healthcare organizations handle huge amounts of sensitive health records and share data with others. Our audit system watches over all this data movement and access carefully.

Automation tools help improve our compliance management. They check workers' vaccination status and change entry rules based on state regulations. This makes record-keeping more accurate and needs less manual oversight.

We stay ahead of compliance through constant monitoring and security checks. Our integrated system spots security gaps before anyone can exploit them. Network segmentation happens automatically based on our 6-year-old policies. This detailed approach helps us meet today's compliance needs and tomorrow's security challenges in healthcare.

VII. EMPLOYEE TRAINING AND AWARENESS

Training and awareness build the foundation of our healthcare cybersecurity strategy. Our experience shows that security works best when staff members understand their role in protecting patient data and maintaining system integrity.

Security Awareness Programs

Our complete security awareness training addresses unique challenges in healthcare environments. Staff members retain 25-60% more information through online learning methods and need 40-60% less time to complete the training. Several key components structure our programs:

Training Component Focus Area Implementation Method Basic Security Data Protection Interactive Modules HIPAA Compliance Regulatory Requirements Scenario-based Learning Threat Recognition Risk Identification Simulated Exercises Best Practices Daily Operations Hands-on Training Healthcare employees without proper security awareness training make up 24% of the workforce. This makes resilient educational programs vital. Role-specific training addresses the daily challenges healthcare professionals face.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Incident Reporting Procedures

Swift response to security events depends on clear incident reporting protocols. Staff members can report incidents without fear of blame or retribution. Our reporting framework includes these key elements:

- Staff members must start reporting procedures immediately for incidents or near-misses
- Events need accurate and quick documentation
- Submission systems remain available from any location
- Serious incidents follow clear escalation paths
- Staff involved in incidents receive support mechanisms

A telephone hotline system helps report serious incidents that need escalation and immediate investigation. This system maintains rapid response capabilities and ensures proper documentation of security events.

Access Management Training

Building a strong security culture while maintaining operational efficiency drives our access management training. Healthcare organizations handle large amounts of sensitive information. Data security depends on proper access control.

Different areas from emergency rooms to administrative offices face unique cybersecurity challenges. Role-based training programs address specific departmental needs. Our training highlights:

1. Authentication protocols and password management
2. Multi-factor authentication procedures
3. Device security and mobile access
4. Data sharing protocols
5. Emergency access procedures

Regular assessments provide feedback for improvement. Organizations with complete access management training experience fewer security incidents and maintain better compliance with regulatory requirements.

Cybersecurity awareness has become part of our daily operations. Protecting patient data matters as much as hands-on care for patient well-being. Regular communication and ongoing reminders about best practices have created an environment where security consciousness defines our organizational culture.

Learning management systems track employee progress and identify areas needing additional support. This information-driven approach helps tailor training programs to departmental needs while maintaining consistent security standards.

Staff members involved in serious incidents receive counseling and support. We recognize them as 'second victims' who need assistance. High reporting rates and continuous improvement in security practices result from this supportive approach.

Our complete training approach has created a security-conscious workforce that understands cybersecurity's importance and its role in it. Role-specific training and clear communication channels have established a resilient defense against evolving cyber threats in our healthcare environment.

VIII. CONCLUSION

Healthcare cybersecurity needs constant watchfulness as threats keep evolving. Our detailed review of security strategies shows that modern healthcare institutions need multiple layers of defense.

A strong network architecture forms the foundation. This includes proper device authentication, data encryption, and cloud security measures. Live monitoring combined with quick incident response protocols helps catch and stop threats before they affect patient care.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

Medical organizations should focus on these vital security elements:

- Network segmentation and access controls
- Medical IoT device protection
- Detailed data encryption
- Cloud security integration
- Employee security awareness training
- HIPAA compliance management

The core team's training is significant since security-aware employees create the first defense line against cyber threats. Regular security checks, updated documentation, and audit trails show our steadfast dedication to protecting sensitive patient information while following regulations.

Healthcare security goes beyond technical solutions. Organizations need a culture of awareness, responsibility, and continuous improvement. Healthcare organizations can reduce their vulnerability by implementing these strategies properly while running efficiently and providing quality patient care.

REFERENCES

1. **Appari, A., & Johnson, M. E.** (2010). Information security and privacy in healthcare: Current state of research. International Journal of Internet and Enterprise Management, 6(4), 279–314. https://doi.org/10.1504/IJIEM.2010.035624
2. **Benaloh, J., Chase, M., Horvitz, E., & Lauter, K.** (2009). Patient-controlled encryption: Ensuring the privacy of electronic medical records. In Proceedings of the 2009 ACM workshop on Cloud computing security (pp. 103–114). https://doi.org/10.1145/1655008.1655024
3. **Bourgeois, F. C., Taylor, P. L., Emans, S. J., Nigrin, D. J., & Mandl, K. D.** (2008). Whose personal control? Creating private, personally controlled health records for pediatric and adolescent patients. Journal of the American Medical Informatics Association, 15(6), 737–743. https://doi.org/10.1197/jamia.M2799
4. **Carter, J. H.** (2008). Electronic health records: A guide for clinicians and administrators. ACP Press.
5. **Cohen, I. G., & Mello, M. M.** (2018). HIPAA and protecting health information in the 21st century. JAMA, 320(3), 231–232. https://doi.org/10.1001/jama.2018.5630
6. **Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A.** (2013). Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 46(3), 541–562. https://doi.org/10.1016/j.jbi.2012.12.003
7. **Fichman, R. G., Kohli, R., & Krishnan, R.** (2011). Editorial overview—the role of information systems in healthcare: Current research and future trends. Information Systems Research, 22(3), 419–428. https://doi.org/10.1287/isre.1110.0382
8. **Furnell, S., & Warren, M.** (1999). Computer hacking and cyber terrorism: The real threats in the new millennium? Computers & Security, 18(1), 28–34. https://doi.org/10.1016/S0167-4048(99)80006-5
9. **Gellman, R.** (2010). Privacy in the clouds: Risks to privacy and confidentiality from cloud computing. World Privacy Forum.
10. **Goldstein, M. M., & Pewen, W. F.** (2013). The HIPAA omnibus rule: Implications for public health policy and practice. Public Health Reports, 128(6), 554–558. https://doi.org/10.1177/003335491312800611
11. **Harman, L. B., Flite, C. A., & Bond, K.** (2012). Electronic health records: Privacy, confidentiality, and security. Virtual Mentor, 14(9), 712–719. https://doi.org/10.1001/virtualmentor.2012.14.9.stas1-1209
12. **Jalali, M. S., & Kaiser, J. P.** (2018). Cybersecurity in hospitals: A systematic, organizational perspective. Journal of Medical Internet Research, 20(5), e10059. https://doi.org/10.2196/10059
13. **Kierkegaard, P.** (2011). Electronic health record: Wiring Europe's healthcare. Computer Law & Security Review, 27(5), 503–515. https://doi.org/10.1016/j.clsr.2011.07.010
14. **Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A.** (2017). Security techniques for electronic health records. Journal of Medical Systems, 41(8), 127. https://doi.org/10.1007/s10916-017-0778-4

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 2, February 2019

15. **McLeod, A., & Dolezel, D.** (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. Decision Support Systems, 108, 57–68. https://doi.org/10.1016/j.dss.2018.02.007
16. **Menachemi, N., & Collum, T. H.** (2011). Benefits and drawbacks of electronic health record systems. Risk Management and Healthcare Policy, 4, 47–55. https://doi.org/10.2147/RMHP.S12985
17. **Moore, P., & Frye, S.** (2017). Security and privacy in the healthcare environment. HIMSS.
18. **Rindfleisch, T. C.** (1997). Privacy, information technology, and health care. Communications of the ACM, 40(8), 92–100. https://doi.org/10.1145/257874.257896
19. **Smith, H. J., Milberg, S. J., & Burke, S. J.** (1996). Information privacy: Measuring individuals' concerns about organizational practices. MIS Quarterly, 20(2), 167–196. https://doi.org/10.2307/249477
20. **Wager, K. A., Lee, F. W., & Glaser, J. P.** (2017). Health care information systems: A practical approach for health care management (4th ed.). Jossey-Bass.