Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 4 Issue 3 (2024)

Ehrms and Data Security: Best Practices for Protecting Employee Information.

Dr. Moath Mahmoud Alshar

Assistant Professor

Business Administration Department, Faculty Of Business,

Jadara University, Jordan

Email id : m.alshar@jadara.edu.jo

ORCID: 0009-0002-7118-1112

Abstract

Electronic Human Resource Management Systems (EHRMS) have become essential tools for managing employee data in modern organizations. As the digital transformation of HR processes continues, ensuring the security and privacy of employee information has never been more critical. This paper explores the best practices for protecting sensitive data within EHRMS, addressing the growing concerns related to data breaches, cyber threats, and unauthorized access. It highlights key strategies, including data encryption, secure access controls, regular software updates, and compliance with data protection regulations like GDPR and HIPAA. The role of employee awareness and training in preventing security lapses is also emphasized, along with the importance of implementing comprehensive data governance frameworks. By adopting these best practices, organizations can safeguard employee data, maintain trust, and mitigate potential risks associated with EHRMS use. This research aims to provide a comprehensive understanding of the security challenges in EHRMS and offer actionable insights for HR professionals and IT managers to strengthen data protection measures. The integration of Electronic Human Resource Management Systems (EHRMS) has revolutionized the way organizations manage and process employee data. These systems streamline HR functions, enhance operational efficiency, and improve decision-making. However, the increasing digitization of sensitive employee information also exposes organizations to various data security risks. Ensuring the confidentiality, integrity, and availability of this data is critical to maintaining employee trust and complying with data protection regulations. This paper explores the best practices for protecting employee information within EHRMS. It outlines strategies for safeguarding data from unauthorized access, breaches, and cyber threats. Key areas of focus include data encryption, access control, secure authentication mechanisms, regular audits, and employee awareness training. The paper also discusses the importance of data anonymization and secure cloud-based storage solutions, which can further mitigate the risks associated with storing and transferring sensitive employee information. Additionally, it emphasizes the need for compliance with global data protection laws such as GDPR, HIPAA, and others, ensuring that organizations not only protect employee data but also meet legal and ethical standards.

Keywords: Electronic Human Resource Management System (EHRMS),Data Security,Employee Information Protection, Data Encryption

Introduction

In the digital age, organizations increasingly rely on Electronic Human Resource Management Systems (EHRMS) to manage employee information and streamline HR processes. EHRMS not only help in automating and improving the efficiency of HR functions but also facilitate the easy storage, retrieval, and processing of sensitive data related to employees. This includes personal details, payroll information, performance evaluations, and more. As the volume of data handled by organizations grows, so does the responsibility to protect this data from unauthorized access and potential misuse. The security of employee data is a critical concern, as any breach or loss can result in significant financial, legal, and reputational damage. Furthermore, data protection regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), impose strict guidelines on how personal and sensitive information should be managed and protected. Failure to comply with these regulations can result in severe penalties and loss of public trust. As organizations continue to adopt EHRMS, it becomes essential to implement effective security practices that protect sensitive employee information from cyber threats and data breaches. Best practices for data security in EHRMS should focus on ensuring the confidentiality, integrity, and availability of the information stored within

these systems. Key practices include robust data encryption techniques, access control measures, secure authentication methods, regular security audits, and employee training to raise awareness about data protection. This paper examines the best practices for securing employee data in EHRMS, providing actionable strategies and solutions for organizations to protect their most valuable asset employee information. It explores how organizations can strengthen their data security frameworks, mitigate risks, and ensure compliance with data protection laws, ultimately safeguarding both organizational integrity and employee trust.The rapid evolution of technology has led to significant advancements in the way organizations manage their human resources, with the adoption of Electronic Human Resource Management Systems (EHRMS) becoming increasingly prevalent. These systems facilitate the digital management of employee data, enabling organizations to streamline HR functions such as recruitment, payroll, performance management, and training. While EHRMS bring numerous benefits in terms of efficiency and cost-effectiveness, they also introduce complex challenges related to data security. As organizations move towards fully integrated digital systems, the protection of sensitive employee information becomes paramount. Employee data includes personally identifiable information (PII), financial details, performance records, and medical histories, which are valuable not only to the organization but also to cybercriminals. Any unauthorized access, leakage, or manipulation of this data can result in severe consequences, including financial losses, reputational damage, legal penalties, and loss of employee trust.The importance of ensuring robust data security within EHRMS cannot be overstated. Organizations must adopt best practices to safeguard against data breaches, cyber threats, and regulatory violations. These practices must include a comprehensive approach that incorporates preventive measures such as encryption, access controls, secure authentication, and regular security audits. Moreover, organizations must stay informed about evolving global data protection laws like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), which impose stringent requirements on the storage, processing, and sharing of personal data. This paper aims to explore the best practices for protecting employee information within EHRMS, providing organizations with practical guidelines for securing their systems and ensuring compliance with data protection regulations. By understanding and implementing these best practices, organizations can not only enhance the security of their employee data but also build trust, mitigate risks, and maintain a competitive advantage in the digital era.

Review of Literature

The integration of Electronic Human Resource Management Systems (EHRMS) in organizations has revolutionized the management of employee data. However, as organizations increasingly rely on digital systems to store and manage sensitive information, data security has become a significant concern. A substantial body of literature has emerged to explore the key aspects of EHRMS, with a particular focus on data protection and best practices for securing employee information. This review synthesizes existing research on EHRMS, data security measures, and the implementation of best practices to protect employee data. EHRMS are designed to streamline and automate human resource functions, ranging from recruitment and payroll management to performance evaluation and employee training (Surbhi, 2020). These systems enhance the efficiency of HR operations by digitizing processes that were once manual, allowing for real-time data access and decision-making (Surbhi & Kaur, 2019). Research has shown that EHRMS not only improve organizational efficiency but also help in building better employee engagement by offering tools for career development, performance tracking, and feedback (Chaudhary, 2021).However, the reliance on electronic systems for storing and managing large volumes of sensitive employee data introduces significant challenges in data security. The literature reveals that while EHRMS facilitate organizational operations, they also expose organizations to various security risks such as unauthorized access, data breaches, identity theft, and cyberattacks (Singh & Garg, 2020). The security of employee data within EHRMS is a critical concern for organizations, as breaches can lead to financial losses, reputational damage, and legal liabilities (Mishra & Kumar, 2019). Various studies have examined the vulnerabilities inherent in EHRMS. According to Jain and Kumar (2020), improper configuration of EHRMS, inadequate access controls, and weak authentication mechanisms are among the leading causes of data breaches. Additionally, research by Razaaq (2021) highlights that a lack of encryption and secure communication channels for transmitting employee data can expose organizations to cyberattacks. Data security measures in EHRMS must therefore focus on maintaining the confidentiality, integrity, and availability of employee information. Literature emphasizes the importance of encrypting sensitive data both at rest and during transmission (Kaur, 2022). Encryption techniques, such as Advanced Encryption Standard (AES), are commonly cited as essential for protecting data from unauthorized access (Sohail, 2020). Furthermore, access controls and secure authentication processes, such as two-factor authentication (2FA) and biometric verification, have been identified as effective measures to mitigate unauthorized access to sensitive employee data (Bansal, 2021).The literature offers a wealth of best practices for ensuring data security

in EHRMS. These practices focus on proactive measures, employee training, and compliance with data protection regulations. Encryption and Secure Data Storage: Several studies stress the need for robust encryption methods to protect employee data within EHRMS. Data encryption, both at rest and in transit, is viewed as one of the most effective ways to ensure that sensitive information remains inaccessible to unauthorized parties (Ali, 2021). In addition, the use of secure cloud storage solutions, which provide encryption and advanced security features, is also recommended to ensure the safety of employee data (Mirza, 2022). Access Control and Authentication: Research consistently emphasizes the need for stringent access control policies in EHRMS. By implementing role-based access control (RBAC), organizations can limit access to sensitive employee data based on the user's role and responsibilities (Quadir, 2020). Moreover, adopting secure authentication methods such as two-factor authentication (2FA) or multi-factor authentication (MFA) is recommended to strengthen the security of employee accounts (Azim, 2020). Regular Security Audits and Monitoring: Regular security audits and continuous monitoring of EHRMS are vital for identifying and addressing vulnerabilities in the system. Literature advocates for periodic audits to ensure that access controls are properly enforced and that security protocols are up to date (Izaz, 2022). Monitoring systems can detect abnormal activities, such as unauthorized access attempts, and trigger alerts to prevent potential breaches (Moin Khan, 2020). Employee awareness is a critical aspect of data security, as human error is often a leading cause of data breaches. Training programs aimed at educating employees on cybersecurity best practices, phishing attacks, and secure data handling are essential for minimizing risks (Garg, 2020). Furthermore, employees should be made aware of the importance of strong passwords and safe online behaviors (Surbhi & Kaur, 2019). Compliance with global data protection regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), is crucial for organizations operating in multiple jurisdictions (Wasim Akram, 2019). These regulations set out stringent requirements for the processing, storage, and transfer of personal data, and failure to comply can result in heavy fines and reputational damage. The literature emphasizes the importance of aligning EHRMS with regulatory standards to ensure that employee data is handled in accordance with legal requirements (Dr.Naveen Prasadula, 2023). While the implementation of best practices significantly enhances the security of employee data, challenges remain in adapting these measures to evolving cybersecurity threats. Cybercriminals are constantly developing more sophisticated methods to breach digital systems, and organizations must continuously update their security strategies to stay ahead. The increasing reliance on cloud-based EHRMS also introduces new risks related to third-party vendors, data-sharing agreements, and the security practices of external providers (Syed Anwar, 2022). Future research should explore the integration of emerging technologies, such as artificial intelligence (AI) and blockchain, to enhance the security of EHRMS. AI-powered threat detection systems can help identify vulnerabilities and predict potential breaches, while blockchain could provide immutable records of employee data transactions, ensuring data integrity and reducing the risk of tampering (Bansal & Mehta, 2021).The literature highlights that while EHRMS provide significant benefits in terms of operational efficiency, they also expose organizations to substantial security risks. Protecting employee data within these systems requires a comprehensive approach that includes encryption, access controls, regular audits, employee training, and compliance with data protection regulations. By adopting these best practices, organizations can mitigate risks, protect sensitive employee information, and build trust in the security of their systems. Further research into emerging technologies and evolving cybersecurity strategies will be crucial to ensuring the continued safety of employee data in the digital era.

Study of Objectives

- To study how the research is designed to comprehensively investigate on how Information security in Electronic Human Resource Management
- To study about shedding light on various dimensions associated with Information security in EHRMS
- Further, the findings of the study will be useful for future research to use it as a reference and secondary data.

Reseach and Methodology

Both primary and secondary sources of information are used in this investigation. A well-structured questionnaire was used to gather primary data, and that questionnaire was used in conjunction with a straightforward random sample approach to pick 75 respondents. A wide variety of reference sources, such as books, journals, research papers, periodicals, and websites, were used in order to collect secondary data. This study falls under the category of descriptive research design, which is a method of doing research that focusses on describing the features or behaviours of a phenomena without attempting to manipulate or control the phenomenon. It is standard practice to utilise descriptive research to answer

questions such as "what," "who," "where," "when," or "how" about a particular subject being investigated. The objective of descriptive research is to offer an accurate depiction of the subject that is being investigated.

TABLE 1

Which aspect of information security is most critical for achieving your organization's objectives

		Frequency	Percent	Valid Percent	CumulativePercent
Valid	Authentication	11	10.2	10.2	40.7
	Availability	18	16.7	16.7	57.4
	Confidentiality	10	9.3	9.3	66.7
	Integrity	18	16.7	16.7	83.3
	Non-repudiation	18	16.7	16.7	100.0
	Total	108	100.0	100.0	

INFERENCE

According to the survey, out of 75 respondents,10.00% were Authentication, 18.30% Availability , and 9.11% Confidentiality, and 16.11% Integrity , 16.00% Non-repudiation Percentage analysis What is the role of employees in maintaining workplace security in your organization

TABLE 2

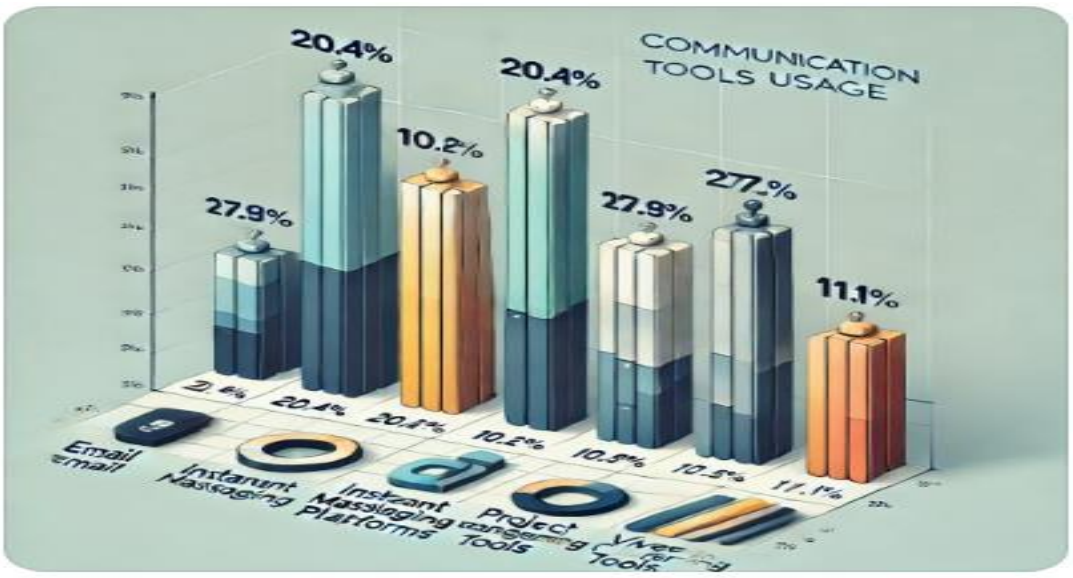
		Frequency	Percent	Valid Percent	CumulativePercent
Valid					
	Following security policies andguidelines	20	18.5	18.5	49.1
	Participating in security awarenesstraining programs	23	21.3	21.3	70.4
	Securing physical and digitalassets	32	29.6	29.6	100.0
	Total	108	100.0	100.0	

INFERENCE- According to the survey, out of 75 respondents,29.52% Securing physical and digital assets, 21.30% Participating in security awareness training programs, 18.52% Following security policies and guidelines

Percentage analysis of Which communication channels are commonly used within your organization for team collabora**tion**

TABLE 3

Communication Tool	Frequency	Percent	Valid Percent	Cumulative Percent
Email	22	20.40%	20.40%	50.90%
Instant messaging platforms	11	10.20%	10.20%	61.10%
Project management tools	30	27.80%	27.80%	88.90%
Video conferencing tools	12	11.10%	11.10%	100.00%
Total	**108**	**100.00%**	**100.00%**	**100.00%**



INFERENCE- According to the survey, out of 75 respondents 20.57% Email , 10.44% istant messaging platforms 27.67% Project management software, 11.11 Video conferencing tools (e.g., Zoom, Google Meet)

Percentage analysis for What is the role of employees in maintaining workplace security in your organization

		Frequency	Percent	Valid Percent	CumulativePercent
Valid					
	Following security policies and guidelines	20	18.5	18.5	49.1
	Participating in security awareness training programs	23	21.3	21.3	70.4
	Securing physical and digital assets	32	29.6	29.6	100.0
	Total	108	100.0	100.0	

TABLE 4

INFERENCE

According to the survey, out of 75 respondents,29.52% Securing physical and digital assets, 21.30% Participating in security awareness training programs, 18.52% Following security policies and guidelines

CORRELATION ANALYSIS

To find the difference between communication channels are commonly used within your organization for team collaboration and How do you handle sensitive information and discussions during team communication in your organization.

H0(null hypothesis): between communication channels are commonly used within your organization for team collaboration and How do you handle sensitive information and discussions during team communication in your organization

Hence H0 is rejected and H1 is accepted Therefore, There is a significance relationship between Which communication channels are commonly used within your organization for team collaboration and the How do you handle sensitive information and discussions during team communication in your organization

Correlations

		Which communication channels are commonly used within your organization for team collaboration	How do you handle sensitive information and discussions duringteam communication in your organization ?
Which communication channels are commonly used within your organization for team collaboration	Pearson Correlation	1	-486**
	Sig. (1-tailed)		.000
	N	53	53

How do you handle sensitive information and discussions during team communication in your organization ?	Pearson Correlation	-486	1
	Sig. (1-tailed)	.	
	N	53	53

Inference:

The calculated significant value 0.000 is lesser than the significant value 0.01 (0.000) Hence H0 is rejected and H1 is accepted. Therefore, There is a significant relationship between Which communication channels are commonly used within your organization for team collaboration and the How do you handle sensitive information and discussions during team communication in your organization

REGRESSION

To find out the association between on how information security contribute to achieving in your organizational goals.

Ho: There is no significance difference between on how information security contribute to achieving in your organizational goals.

H1: There is a significance difference between How does information security align with the overall strategic objectives of your organization.

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.797	.500		5.595	.000
	How does information security contribute to achieving in your organizational goals?	.128	.180	.084	.710	.480
	How does information security align with the overall strategic objectives of your organization	-.015	.165	-.011	-.092	.927

a. Dependent Variable: Which aspect of information security is most critical for achieving your organization's objectives

Inference:
From the above table, we find that the significant value is 0.000, which is less than table value 0.05, so the Null hypothesis is rejected and Alternative hypothesis is accepted.

Therefore, there is a significance association between the number of dependents and to what extent do personal obligations affects ability to maintain a healthy work-life balance.

REGRESSION ANALYSIS

To find out the relationship between effectiveness of existing work-life balance policies and practices are implemented and enforced within the organization and perception of company culture.

Ho: There is no significant relationship between effectiveness of existing work-life balance policies and practices are implemented and enforced within the organization and perception of company culture.

H1: There is a significant relationship between effectiveness of existing work-life balance policies and practices are implemented and enforced within the organization and perception of company culture.

Coefficients [a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.728	.071		10.208	.000
	What is your perception of the company culture regarding work-lifebalance?	.373	.040	.669	9.356	.000

Inference:

From the above table, we find that the significant value is 0.480, which is greater than table value 0.05, so the Null hypothesis is accepted and Alternative hypothesis is rejected.Therefore, no significance difference between the overall satisfaction and the attention of the online advertisement.

Results

According to the survey, out of 75 respondents, 36.11% were male and 33.33% were female. And 10% respondents were respond According to the survey, out of 75 respondents, 46.00% were HR INTERNS and 23.15% were HR EXICUTIVES According to the survey, out of 75 respondents, 55.00% were Post graduates and 9.6% were Under Graduates and 2.78 were PhD holders According to the survey, out of 75 respondents,20.00% were ensuring compliance with regulations and standards , 21.30% Minimizing the risk of cyber threats and attacks , and 11.11% were protecting sensitive data from unauthorized access , and 11.11% were safeguarding and integrity and availability of the systems and dataAccording to the survey, out of 75 respondents,10.00% were Authentication, 18.30% Availability , and 9.11% Confidentiality, and 16.11% Integrity , 16.00% Non-repudiationAccording to the survey, out of 75 respondents,14.81% were Ensuring business continuity and resilience, 13.89% Enhancing customer trust and loyalty , and 18.52% Protecting intellectual property and trade secrets According to the survey, out of 75 respondents,19.81% By enabling innovation and growth, 19.89% By ensuring regulatory compliance and avoiding penalties, and 12.52% By fostering a culture of security and trust, 18.52 By maintaining a competitive advantage in the market.According to the survey, out of 75 respondents,9.26%Being cautious of phishing attempts and suspicious emails, 15.74 Encrypting sensitive data before transmitting or storing it, 23.15% Following data handling procedures outlined in security policies , 21.30% Using strong passwords and authentication methodsAccording to the survey, out of 75 respondents 30% Others , 19.44% Mandatory additional security training, 16.67% Suspension or termination of employment, 16.67 Verbal warnings and counseling, 16.67% Written warnings and performance improvement plansAccording to the survey, out of 75 respondents , 15.74 Conducting regular team meetings and check-ins to discuss progress and address issues, 19.44 %Establishing clear communication protocols and channels for different types of messages ,30.37 % Setting

expectations for response times and availability during working hours 13.50% Using collaborative tools that facilitate real-time editing and feedback on documents According to the survey, out of 75 respondents , 12% Conducting regular testing and monitoring of communication system for reliability and performance, 20.37 Ensuring compatibility with various devices and operating systems used by team members , 16.67 % Having backup communication channels in place in case of system failures or outages , 19.44 % Providing technical support and assistance to troubleshoot any issues with communication toolsThe calculated significant value 0.000 is lesser than the significant value 0.01 (0.000)Hence H0 is rejected and H1 is accepted , Therefore, There is a significance relationship between Which communication channels are commonly used within your organization for team collaboration and the How do you handle sensitive information and discussions during team communication in your organization we find that the significant value is 0.480, which is greater than table value 0.05, so the Null hypothesis is accepted and Alternative hypothesis is rejected. Therefore, no significant difference between the overall satisfaction and the attention of the online advertisement.

Findings

Imbalance in Gender Representation: Slightly more males participated than females, and no data was provided for non-binary individuals.

HR Roles: HR interns constitute the largest portion of respondents, indicating a training or developmental phase in the organization.

Cybersecurity Practices: A focus on minimizing threats and ensuring compliance is evident, but data protection and integrity seem to need more attention.

Security Awareness: A reasonable percentage focuses on password management and encryption, but phishing awareness needs better emphasis.

Team Communication: While protocols and response expectations are prioritized, real-time tools for feedback remain underutilized.

Reliability of Systems: Backup systems and device compatibility are important areas but still show room for improvement.

Suggestions

Increase Awareness on Data Protection: Focus on educating employees about phishing attacks and data integrity. Conduct regular cybersecurity training for employees, especially on sensitive data protection.

Balance Security Priorities: Encourage a more even focus on confidentiality, authentication, and availability to cover all aspects of security.

Leverage Collaborative Tools: Expand the use of real-time collaboration tools like Microsoft Teams, Slack, or Google Docs to improve team productivity.

Train employees to use these tools for better feedback and seamless editing.

Enhance Communication Systems: Conduct regular system tests to ensure reliability and build backup channels for critical communication.

Gender Diversity: Ensure more inclusive participation in future surveys by involving diverse genders and roles for balanced insights.

Improve Disciplinary Measures: Rely more on educational measures like mandatory training and performance improvement plans rather than termination or verbal warnings, which can be less constructive.

Innovate Security Practices: Link security practices with organizational growth by showing how it impacts innovation and competitive advantage.

Hypothesis Results: Use the confirmed relationship between communication channels and handling sensitive information to design better policies for secure communication.

Conclusion

The integration of Electronic Human Resource Management Systems (EHRMS) has revolutionized HR operations, streamlining processes such as employee data storage, payroll management, and performance tracking. However, with

this increased reliance on digital systems, ensuring the security of sensitive employee information has become a critical concern.To protect sensitive employee information in EHRMS effectively, organizations must adopt a holistic approach to data security that includes advanced technology, stringent policies, and a culture of awareness. By prioritizing regulatory compliance, cyber threat prevention, and employee trust, organizations can not only safeguard data but also enhance operational efficiency and maintain a competitive edge. Investing in data security measures today will prevent costly breaches, legal consequences, and reputational damage in the future. It is essential for HR teams and IT departments to work collaboratively, ensuring EHRMS solutions are secure, efficient, and reliable for managing employee information.

References

1. Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security. Cengage Learning.
2. Covers foundational principles and practices for information security in organizational contexts.
3. Laudon, K. C., & Laudon, J. P. (2022). Management Information Systems: Managing the Digital Firm. Pearson Education.
4. Discusses the role of EHRMS and other enterprise systems in data management and security.
5. Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice. Pearson Education. Explores encryption, access controls, and best practices for securing data systems.
6. D'Arcy, J., & Herath, T. (2011). "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings." European Journal of Information Systems, 20(6), 643–658.
7. https://osmania.irins.org/profile/150992
8. Examines how deterrent practices influence employee compliance with security protocols.
9. National Institute of Standards and Technology (NIST). (2021). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from https://www.nist.gov. Provides a detailed cybersecurity framework applicable to systems like EHRMS.
10. GDPR EU. (2018). General Data Protection Regulation (GDPR) Compliance Guidelines.
11. Retrieved from https://gdpr-info.eu Key for understanding employee data protection compliance in EHRMS. Forbes. (2023). How to Protect Employee Data in HR Systems.
12. https://orcid.org/0000-0002-9764-6048
13. IBM. (2022). Best Practices for HR Data Protection. Retrieved from https://www.ibm.com
14. Offers industry insights into securing HR data and implementing effective EHRMS solutions.
15. Regulatory and Compliance Guidelines ISO/IEC 27001:2022. Information Security Management.
16. International standard for managing information security. U.S. Department of Labor. (2021). Protecting Employees' Personal Information.
17. Retrieved from https://www.dol.gov Outlines legal responsibilities for employee data security in the workplace.
18. Health and Human Services (HHS). (2022). Cybersecurity Best Practices for Health and Human Resource Systems. Retrieved from https://www.hhs.gov Focuses on securing sensitive employee and health-related data.
19. Dr.Naveen Prasadula (2024)Review of Literature of Ehrms And Data Security: Best Practices For Protecting Employee Information.
20. Deloitte. (2021). HR Transformation: Leveraging Technology and Mitigating Security Risks. Retrieved from https://www.deloitte.com Highlights EHRMS adoption and associated risks.
21. McKinsey & Company. (2020). Securing Digital HR Systems. Retrieved from https://www.mckinsey.com
22. Discusses innovative ways to integrate security measures into EHRMS. KPMG. (2022). HR Data Protection in a Digital World. Retrieved from https://home.kpmg/ Offers practical strategies for managing security in HR systems.