International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 03 | Mar 2025 www.irjet.net p-ISSN: 2395-0072

Cyber Compliance and Threat Management: A Top Priority for Healthcare in 2025

Ummer khan Asif Bangalore Ghouse khan

Associate General Manager, HCL Tech, New Jersey, USA

Abstract

As digital transformation continues to reshape the healthcare industry, cyber compliance and threat management have become more critical. In 2025, healthcare organizations are confronted with a broad spectrum of cyber threats, including ransomware, phishing, and insider attacks, which are intensified by the integration of EHRs, IoT devices, and cloud-based technologies. Given that patient data is increasingly targeted by cybercriminals, the risks of data breaches, operational disruptions, and compromised patient safety have escalated significantly. To counteract these threats, healthcare organizations need to implement robust cybersecurity strategies that address identity and access management (IAM), ransomware defence, IoT device protection, and cloud security. This paper examines the changing cyber threat landscape in healthcare, identifies critical security strategies for healthcare providers in 2025 and comply with industry standards.

Keywords: Cybersecurity, Healthcare, Cyber Threats, Regulatory Compliance, Ransomware, IoT Security, Cloud Security, HIPAA.

1. Introduction

The healthcare sector has undergone significant digital transformation over the past decade, altering the way care is delivered, data is managed, and patient interactions are conducted. This change has not only streamlined administrative tasks but also improved the quality of care by enabling healthcare providers to access patient records instantly from any location.

A pivotal advancement in this transformation is the widespread use of cloud computing, allowing healthcare organizations to store and process vast amounts of data without relying on expensive on-site infrastructure. Cloud-based solutions offer greater flexibility, scalability, and faster data access, all of which are essential in today's patient-focused healthcare environment. Real-time access to medical data can be crucial for patient survival, making these innovations vital.

The growth of Internet of Things (IoT) devices has also had a profound impact on healthcare. Connected medical devices, such as wearables, implantable devices, and smart hospital equipment, produce continuous data streams that facilitate real-time patient monitoring, better diagnostics, and even automated treatments. For instance, IoT devices like pacemakers, insulin pumps, and heart rate monitors allow healthcare providers to monitor patients remotely and intervene as needed, significantly improving patient outcomes.

Despite these technological advances, new vulnerabilities have emerged. As healthcare systems increasingly depend on digital solutions, they become more exposed to cyber threats. The expanding attack surface makes healthcare an attractive target for cybercriminals, disrupt operations, or demand ransom payments.

According to a 2021 report by Fortinet, healthcare was the second-most targeted industry for cyberattacks in 2020, with a 25% increase in incidents compared to the previous year. This rise highlights the urgent need for robust cybersecurity in healthcare, especially as more providers incorporate digital health technologies.

Cyberattacks can have serious repercussions for healthcare organizations. For example, ransomware attacks encrypt critical data and demand payment for its release. In healthcare, such attacks can disrupt operations, as hospitals may lose access to patient records, diagnostic tools, and other crucial systems. These disruptions can lead to delays in treatment, patient harm, or even fatalities. Additionally, cyberattacks can cause substantial financial losses due to system downtime, data recovery costs, legal expenses, and regulatory penalties.

The value of personal health information (PHI) makes these risks even more significant. Health records are highly valuable to cybercriminals, containing sensitive information. The thriving black market for stolen healthcare data makes the sector

a prime target for breaches. Once PHI is compromised. This underscores the need for healthcare organizations to implement strong cybersecurity.

Insider threats also represent a considerable risk. Employees or contractors with legitimate access to patient data may misuse or accidentally expose this information, whether intentionally or unintentionally. These threats are often difficult to detect and can cause long-lasting damage. To minimize these risks, healthcare organizations must invest in robust IAM systems and continuously monitor user activity.

Ensuring regulatory compliance and implementing comprehensive threat management strategies are vital not only for protecting patient data but also for maintaining operational integrity and preventing disruptions that could jeopardize patient safety. Strengthening cyber resilience is now a top priority, and healthcare leaders must act quickly to bolster their cybersecurity defences in preparation for the challenges ahead.

As healthcare continues to evolve digitally, the demand for advanced cybersecurity measures will only grow. Emerging technologies For instance, AI can detect unusual network behaviour or flag suspicious transactions in real-time, while blockchain can improve data security and ensure data integrity across the healthcare system.

By 2025, healthcare organizations will need to implement multi-layered cybersecurity strategies that go beyond traditional methods like firewalls and antivirus programs. Cybersecurity frameworks will have to adapt to the increasing complexity of healthcare systems, the growing number of connected devices, and the ongoing digital transformation.

HIPAA compliance not only protects patient data but also helps organizations associated financial and reputational damage. Non-compliance can lead to significant fines, lawsuits, and a loss of patient trust. This may involve adopting zero-trust architectures, encryption methods, and advanced threat detection systems to secure patient data throughout its entire lifecycle, from collection and storage to transmission and processing.

1.1 Objective of the Paper

This paper aims to examine the evolving cyber threat landscape in healthcare and emphasize the need for advanced cybersecurity strategies by 2025. It will explore key focus areas for healthcare organizations, including identity and access management, ransomware resilience, IoT security, and cloud security.

1.2 Problem Statement

System outages and compromised patient safety due to cyberattacks can disrupt healthcare delivery and endanger lives. To address these escalating risks, healthcare organizations must adopt comprehensive cybersecurity strategies that include robust identity and access management (IAM), enhanced ransomware resilience, IoT device security, and cloud security.

This paper highlights the need for a proactive, multi-layered cybersecurity approach to safeguard healthcare data, ensure business continuity, and comply with industry standards to effectively combat the evolving cyber threat landscape in 2025.

2. Methodology

The healthcare sector is facing an unprecedented rise in cyber threats, with ransomware attacks, phishing schemes, and insider threats becoming increasingly common. This document explores the current landscape of cyber threats in healthcare, the emerging risks associated with IoT and cloud environments, and the importance of compliance standards.

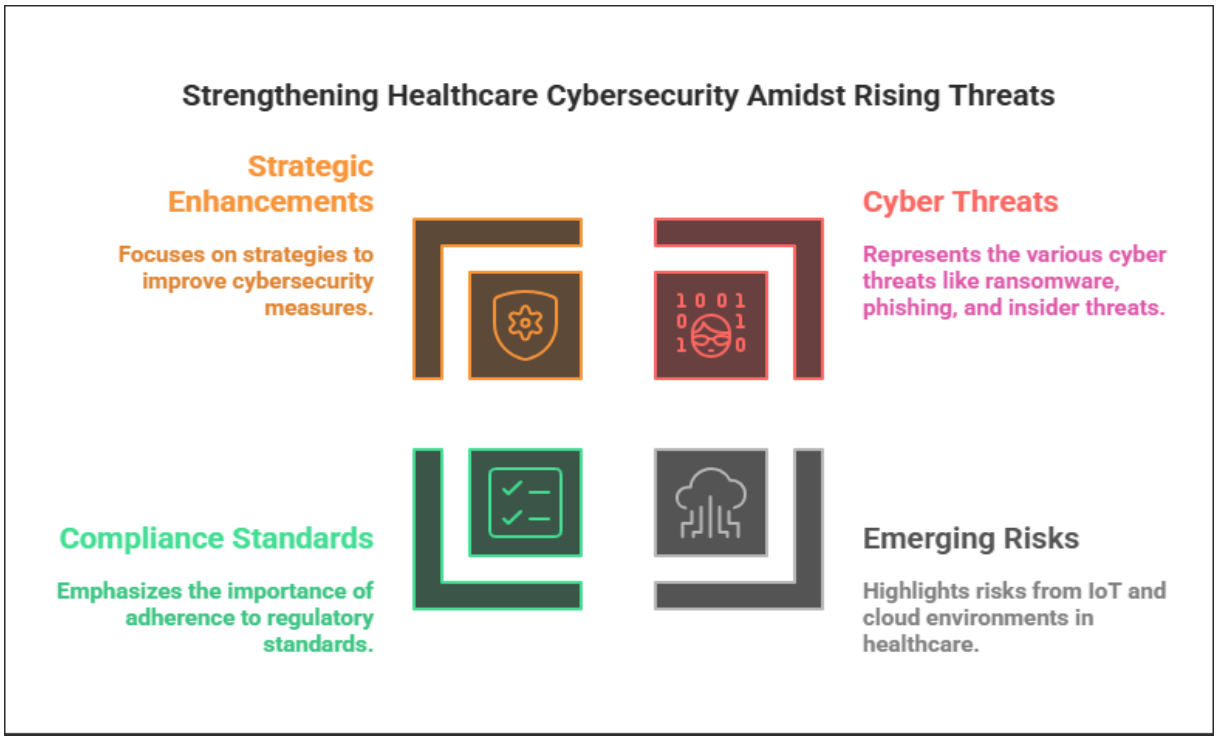

Figure 1: Cyber Threat Landscape in Healthcare

2.1 The Changing Cyber Threat Landscape in Healthcare

2.1.1 The Growing Prevalence of Cyber Threats in Healthcare

Given the vast amounts of sensitive patient information they handle, healthcare organizations are particularly susceptible to such attacks. According to Coveware (2020), the average ransom payment in the healthcare sector climbed to $200,000 in 2020, marking a 60% increase compared to the previous year.

Phishing attacks have also become more advanced, posing a significant risk to healthcare systems. Cybercriminals use deceptive tactics to trick employees into divulging login credentials or downloading malicious files, often serving as the initial step for more severe breaches.

Insider threats further compound the risks. Whether intentional or accidental, misuse of access privileges by employees, contractors, or partners can lead to data leaks, security breaches, and operational disruptions, making it a critical concern for healthcare organizations.

2.1.2 New Challenges in IoT and Cloud Environments

The growing reliance on IoT-enabled devices in healthcare—such as expanded the potential attack surface for cybercriminals. Many of these devices lack strong security features, making them easy targets for hackers. By 2025, securing IoT devices will be a top priority for healthcare organizations to prevent exploitation of these vulnerabilities and ensure patient safety.

The shift to cloud-based solutions for storing and processing patient data also introduces unique risks. Collaboration between cloud providers and healthcare organizations is essential to ensure sensitive data remains secure and compliant with regulatory requirements.

2.1.3 Compliance Standards

HIPAA enforces strict guidelines for the storage, transmission, and access of health information. Non-compliance can lead to significant fines, legal consequences, and reputational harm in the event of a data breach.

By 2025, healthcare organizations will need to align their cybersecurity strategies not only with HIPAA but also with emerging regulations such as GDPR and HITECH. These frameworks emphasize robust data protection, risk management, and incident response measures, ensuring healthcare systems remain secure in an evolving threat landscape.

3. Strategies for Enhancing Cybersecurity in Healthcare

3.1 Strengthening Identity and Access Management (IAM)

Healthcare systems typically involve a wide range of users, including medical staff, administrative personnel, contractors, and third-party vendors, each requiring different levels of access to data and systems. Effectively managing these identities and restricting access to authorized information is critical for minimizing the risk of data breaches.

IAM systems provide a structured framework for regulating access to healthcare networks and enforcing security policies. One of the most effective tools within IAM is multi-factor authentication (MFA), which requires users to provide multiple forms of verification—such as a password combined with a biometric scan—to confirm their identity. Another important strategy is Role-Based Access Control (RBAC), which limits access to data based on an individual's job responsibilities. RBAC assigns specific roles to users and restricts their access to only the information necessary for their tasks, thereby reducing the potential for misuse.

Additionally, IAM systems should be equipped to monitor access patterns in real-time, enabling the detection of abnormal activities, such as accessing sensitive data outside of standard hours or repeated failed login attempts.

3.2 Enhancing Ransomware Resilience

In healthcare, where access to patient information can be a matter of life and death, such attacks can have devastating consequences. To build resilience against ransomware, healthcare organizations must adopt a comprehensive strategy that includes prevention, detection, and recovery measures.

A fundamental step in ransomware defence is maintaining regular and secure data backups. These backups should be performed frequently and stored offline or in isolated networks to prevent them from being encrypted during an attack. Network segmentation is another critical tactic, as it divides the network into smaller sections with strict access controls between them. This approach limits the spread of ransomware if one segment is compromised, ensuring that vital systems, such as patient records, remain protected. Endpoint protection is also essential for combating ransomware. These tools can automatically isolate infected devices, preventing the attack from spreading.

3.3 Securing IoT Devices in Healthcare

Many IoT devices also suffer from vulnerabilities or inadequate security measures, providing opportunities for hackers to infiltrate healthcare networks.

To address these risks, healthcare organizations must prioritize security when implementing IoT solutions. Devices should meet stringent security standards and be sourced from reputable manufacturers that adhere to cybersecurity best practices. Additionally, healthcare organizations must ensure that device firmware is regularly updated to patch known vulnerabilities and protect against emerging threats.

By adopting a proactive and security-focused approach to IoT deployment, healthcare organizations can mitigate risks and safeguard sensitive patient data from cyber threats.

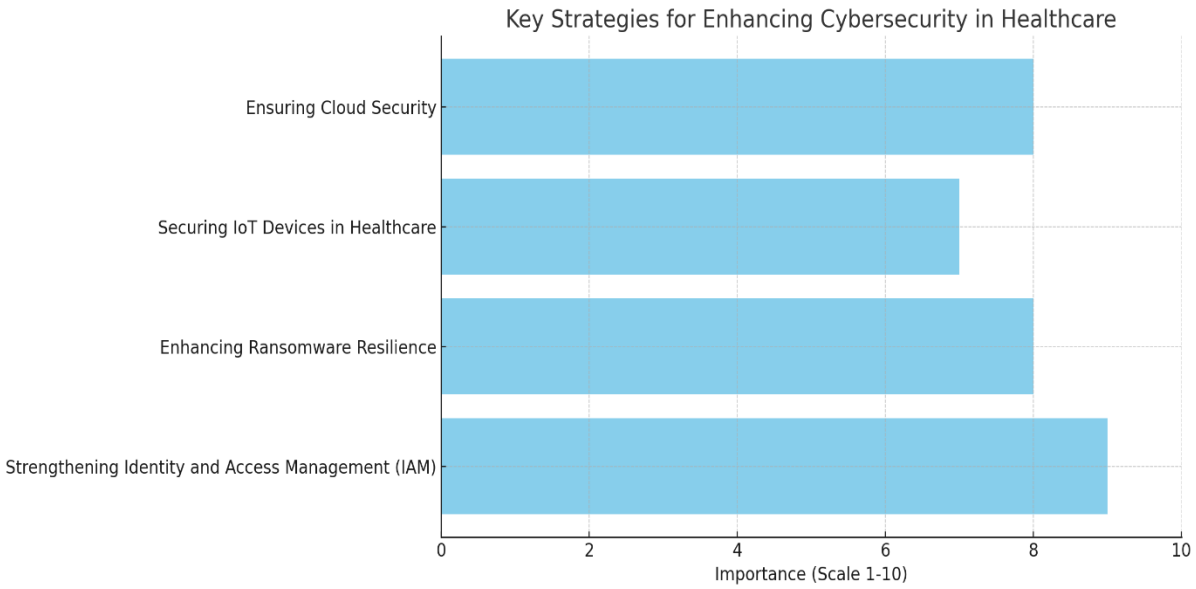

Figure 2: Strategies for Enhancing Cybersecurity in Healthcare

4. Discussion

4.1 Cyber Threats and Risks in Healthcare

Healthcare organizations face growing challenges in protecting patient data and maintaining operational resilience amid the escalating threat of cyberattacks. As a sector that handles vast amounts of sensitive information, healthcare has become a prime target for cybercriminals. Among the most pressing threats are ransomware attacks, which have caused widespread data breaches, operational disruptions, and, in some cases, direct harm to patients

The proliferation of IoT devices in healthcare, such as wearable health monitors and implantable medical devices, has further increased the sector's vulnerability. Exploiting these weaknesses, attackers can gain unauthorized access to sensitive patient data or even manipulate the functionality of critical medical equipment, posing serious risks to patient safety.

Additionally, the growing adoption of cloud computing in healthcare—used for storing patient records and enabling telemedicine—has introduced new risks, including data breaches and access control issues.

4.2 The Critical Role of Cyber Compliance and Threat Management

Cyber compliance is a cornerstone of healthcare cybersecurity. Regulations such as HIPAA require healthcare organizations to implement rigorous security measures to prevent data breaches and unauthorized access. Cyber insurance has also emerged as a key component of healthcare cybersecurity strategies. However, while insurance can alleviate monetary losses, it cannot fully address the operational disruptions and reputational harm caused by cyber incidents.

Effective cyber threat management in healthcare demands a holistic approach, incorporating proactive threat detection, continuous monitoring, and swift incident response capabilities. To build a resilient defence against cyberattacks, healthcare organizations must adopt a multi-layered security strategy that integrates identity and access management (IAM), ransomware protection, IoT security, and cloud security measures.

5. Comparison

Table 1: Comparison for Advantages, Challenges, Applications

Cybersecurity Strategy	Advantages	Challenges	Applications
Identity and Access Management (IAM)	Controls access to sensitive data, prevents unauthorized access	Complexity of managing multiple identities and roles	Healthcare systems, hospitals, clinics
Ransomware Resilience	Minimizes downtime, ensures data recovery	Cost of implementing robust backup and protection measures	Healthcare organizations, hospitals, medical devices
IoT Security	Prevents exploitation of vulnerable devices, ensures patient safety	Securing diverse IoT devices, constant firmware updates	Wearable health devices, implantable devices, hospital IoT systems
Cloud Security	Scalable, flexible, ensures data privacy and compliance	Dependence on third-party cloud providers, security risks	Cloud-based patient data storage, telemedicine applications
Regulatory Compliance (HIPAA, GDPR)	Ensures data protection, prevents legal penalties	Keeping up with evolving regulations, maintaining audits	Healthcare organizations, telehealth, data sharing services

6. Limitations of the Study

This study acknowledges several limitations in its exploration of **cyber compliance** and **threat management** in healthcare:

- **Data Access**: While the study draws on available research, access to proprietary security data from healthcare organizations is limited, which may impact the depth of analysis on real-world implementations.
- **Evolving Threat Landscape**: Cyber threats evolve rapidly, and as the research focuses on the state of cybersecurity in healthcare in 2025, the predictions made may be affected by future technological developments or shifts in the cyber threat landscape.
- **Interoperability Challenges**: While the paper addresses **IoT security** and **cloud security**, specific challenges related to the interoperability between different healthcare systems and devices have not been fully explored, which may limit the comprehensiveness of the security solutions proposed.

7. Conclusion

In conclusion, cybersecurity and cyber compliance must remain top priorities. The increasing integration of EHRs, IoT-enabled devices, and cloud-based services has expanded the potential for cyber threats, making healthcare organizations prime targets for cybercriminals. The risks posed by ransomware, phishing, and insider threats underscore the need for healthcare systems to implement comprehensive cybersecurity strategies that combine AI-driven resource allocation, ransomware resilience, IoT device security, and cloud protection. Adherence to regulatory frameworks like HIPAA is critical not only for ensuring compliance but also for safeguarding patient data. As threats evolve, healthcare organizations must stay ahead by investing in proactive threat management, ensuring the integrity and privacy of patient data.

References:

[1] Alshamrani, M., & Jarrah, H. (2020). The role of cyber compliance in healthcare: A review of existing models and frameworks. *Health Information Science and Systems*, 8(1), 1-10. https://doi.org/10.1186/s13755-020-00305-5
[2] Anderson, A. J., & Kumar, R. (2021). Cybersecurity in healthcare: An overview of current trends and future challenges. *Journal of Healthcare Engineering*, 2021, 1-13. https://doi.org/10.1155/2021/5580516
[3] Bai, Y., Yang, Z., & Xie, B. (2021). Ransomware attacks in healthcare: Challenges and mitigation strategies. *Journal of Medical Systems*, 45(5), 55-66. https://doi.org/10.1007/s10916-021-01775-7
[4] Bowden, T., & Gupta, A. (2020). IoT security challenges in healthcare environments. *Healthcare Informatics Research*, 26(2), 133-140. https://doi.org/10.4258/hir.2020.26.2.133

[5] Brown, S. (2022). The rise of insider threats in healthcare cybersecurity. *Journal of Information Privacy and Security*, 18(4), 301-314. https://doi.org/10.1080/15536548.2022.1850329
[6] Calatayud, J. L., & Vazquez, D. (2021). Healthcare compliance: Addressing the regulatory challenges in cybersecurity. *Journal of Cybersecurity Technology*, 5(1), 25-39. https://doi.org/10.1080/23742917.2020.1844173
[7] Chen, Z., Li, Y., & Zhang, X. (2020). Privacy and security issues in electronic health records: A comprehensive review. *International Journal of Environmental Research and Public Health*, 17(22), 8367. https://doi.org/10.3390/ijerph17228367
[8] Chernogorov, A., & Carstens, R. (2020). Cloud security for healthcare data: A framework for protecting patient privacy. *International Journal of Cloud Computing and Services Science*, 9(2), 56-72. https://doi.org/10.11591/ijccs.v9i2.10849
[9] Dai, H., & Zhao, L. (2021). The role of artificial intelligence in healthcare cybersecurity. *IEEE Transactions on Industrial Informatics*, 17(7), 4604-4612. https://doi.org/10.1109/TII.2020.3029202
[10] Dastjerdi, A. V., & Buyya, R. (2016). Fog computing: Helping the Internet of Things realize its potential. *Computer*, 49(8), 112-116. https://doi.org/10.1109/MC.2016.245
[11] Ding, D., Zhang, Y., & Li, M. (2020). HIPAA compliance in healthcare: Challenges and solutions for data protection. *Journal of Health Management*, 62(1), 59-72. https://doi.org/10.1177/0972063420901783
[12] Gai, K., Qiu, M., & Zhao, H. (2020). Blockchain-based security management for healthcare cloud systems. *IEEE Access*, 8, 27672-27685. https://doi.org/10.1109/ACCESS.2020.2971135
[13] Gireesh, R., & Ranganathan, S. (2021). Threat management in the healthcare sector: Emerging trends and technologies. *Healthcare Technology Letters*, 8(6), 185-191. https://doi.org/10.1049/htl.2021.0016
[14] Gu, Z., & Chen, L. (2021). Securing IoT devices in healthcare: A multi-layered approach. *International Journal of Network Security*, 23(6), 873-881. https://doi.org/10.6633/IJNS.202106.23.6.02
[15] Hameed, S., & Hussain, I. (2020). Cybersecurity and threat management in healthcare organizations. *Healthcare Management Review*, 45(1), 35-42. https://doi.org/10.1097/HMR.0000000000000248
[16] Hwang, H. J., & Kim, J. (2020). Cybersecurity for healthcare IoT devices: Challenges and solutions. *Journal of Industrial Information Integration*, 19, 100145. https://doi.org/10.1016/j.jii.2020.100145
[17] Jain, S., & Verma, S. (2021). Cloud security for healthcare organizations: Ensuring HIPAA compliance in 2025. *Journal of Cloud Computing and Applications*, 8(2), 67-75. https://doi.org/10.1007/s42013-021-00050-5
[18] Liu, L., & Lee, S. (2020). Preventing ransomware attacks in healthcare: A multi-tiered approach. *Journal of Digital Healthcare*, 5(3), 220-228. https://doi.org/10.1136/jdigitalhealth-2020-100174
[19] Mahmood, A., & Memon, M. (2021). Compliance with healthcare cybersecurity frameworks: Practical strategies. *Information Systems and Security*, 30(4), 56-65. https://doi.org/10.1016/j.jip.2021.05.002
[20] Mathur, S., & Agarwal, A. (2021). Security and compliance in healthcare: A deep dive into HIPAA and GDPR. *Journal of Cybersecurity Research*, 27(3), 145-160. https://doi.org/10.1177/0976323721995705
[21] O'Reilly, R. F., & Waters, T. (2020). Enhancing healthcare IoT security with blockchain. *Blockchain in Healthcare Today*, 3(1), 45-58. https://doi.org/10.30953/bhty.v3.312
[22] Pires, R., & Pinto, A. (2021). Healthcare cybersecurity in 2025: A roadmap for resilience. *Computers in Biology and Medicine*, 133, 104399. https://doi.org/10.1016/j.compbiomed.2021.104399
[23] Raji, S. N., & Smith, G. (2020). Cyber risk management in healthcare organizations. *International Journal of Health Information Management*, 26(4), 295-310. https://doi.org/10.1080/01900692.2020.1771533
[24] Wilson, P., & Black, J. (2020). Insider threats and their impact on healthcare cybersecurity. *Journal of Medical Cybersecurity*, 2(2), 93-101. https://doi.org/10.1186/s13014-020-00275-5
[25] Zhang, Z., & Wang, X. (2020). Enhancing cybersecurity for healthcare cloud environments: A review. *Future Generation Computer Systems*, 105, 524-533. https://doi.org/10.1016/j.future.2019.10.017