ISSN: 2473-4901
v12 n6795

A Healthcare Cloud Readiness Framework: Measuring Technical, Compliance, and Staff Readiness for Cloud Migration

Logan Chaffin
Lcc3013@uncw.edu

Zealia Svecharnik
Zs8464@uncw.edu

Kasey Miller
Millerkc@uncw.edu

University of North Carolina Wilmington
Wilmington, North Carolina, 28403, USA

Abstract

Healthcare organizations face significant pressure to transition their systems to the cloud, yet the journey is often more complex than in many other industries. Challenges such as stringent regulations, outdated infrastructure, and a workforce primarily trained for patient care rather than cloud management can create numerous obstacles. Although various cloud readiness frameworks are available, none are specifically tailored for the healthcare sector. This paper introduces the Healthcare Cloud Readiness Framework (HCRF), a structured assessment tool designed to evaluate an organization's preparedness before embarking on a cloud migration. The framework assesses readiness across three key areas: technical infrastructure and security controls, regulatory compliance, and staff capabilities. Each area is anchored in established standards, including NIST SP 800-53 for security and Bloom's revised taxonomy for workforce development. The outcome is a scored profile that enables organizations to pinpoint their specific gaps and understand what must be addressed prior to migration.

Keywords: Healthcare Cloud Readiness Framework (HCRF), Healthcare Cloud Migration, Cloud Readiness Assessment, HIPAA Compliance, Cloud Security, Cybersecurity Risk Assessment

A Healthcare Cloud Readiness Framework: Measuring Technical, Compliance, and Staff Readiness for Cloud Migration

Logan Chaffin, Zealia Svecharnik, Kasey Miller

1. INTRODUCTION

Healthcare data possesses a unique value that distinguishes it from most other forms of data. An individual Electronic Health Record (EHR) encompasses a patient's diagnoses, prescribed medications, Social Security number, and insurance information, all consolidated into a single repository, and presents risks (Menachemi & Collum, 2011). The decision to transfer such sensitive data to the cloud must be approached with caution, and the migration process is often fraught with challenges, despite the availability of technology to facilitate it, as seen in Terhune (2015).

The proposition of cloud migration within the healthcare sector has been gaining momentum. EHR systems, billing platforms, telemedicine applications, and clinical analytics are increasingly reliant on cloud infrastructure for valid reasons. The scalability and cost-effectiveness afforded by cloud solutions are significant advantages. However, healthcare organizations encounter a distinctive set of challenges not typically faced by other industries. Federal regulations delineate the precise manner in which patient data must be managed, stored, and safeguarded. Furthermore, many organizations continue to operate on legacy systems that were not designed with cloud migration in mind. Additionally, the workforce in these organizations, including physicians, nurses, and administrative personnel, is often overworked and lacks the requisite expertise in information technology (Amod, 2025). Their professional training predominantly focuses on patient care rather than cloud security.

Existing cloud readiness frameworks developed by vendors such as Amazon Web Services and Microsoft, as well as organizations like the Cloud Security Alliance, provide valuable insights but are not specifically tailored for the healthcare industry. These frameworks do not fully address the requirements established by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act, nor do they clarify how the shared responsibility model interacts with obligations regarding electronic Protected Health Information (ePHI). This paper seeks to bridge that gap.

The Healthcare Cloud Readiness Framework (HCRF) offers healthcare organizations a methodology for assessing their readiness across three critical dimensions: technical infrastructure and security, regulatory compliance, and staff capabilities. Each dimension yields a score, which cumulatively forms a comprehensive Healthcare Cloud Readiness Score (HCRS). This score provides organizations with a clear indication of their current standing and identifies areas requiring attention prior to the migration of data. The framework is designed to be actionable, functioning not merely as a checklist but as a scoring model that results in a profile that an organization can meaningfully utilize.

The paper begins by reviewing existing literature on healthcare cloud adoption and cloud readiness assessment, highlighting the limitations of current frameworks when applied to healthcare environments. It then presents the design of the HCRF, including its assessment domains, scoring methodology, and HCRS. To demonstrate its applicability, the framework is retrospectively applied to the Anthem (2015) data breach and the Universal Health Services (2020) ransomware attack. The case studies show that organizations with similar overall readiness scores often exhibit different underlying weaknesses across technical security, regulatory compliance, and workforce preparedness. These findings demonstrate that effective cloud readiness requires a balanced assessment of all three domains and that the HCRF provides healthcare leaders with a practical decision-support tool for identifying remediation priorities before cloud migration.

2. LITERATURE REVIEW

Healthcare organizations have become one of the most frequently targeted sectors for cyberattacks due to the high value of protected health information (PHI), the widespread adoption of interconnected

clinical technologies, and the critical nature of healthcare delivery. Unlike in many industries, cybersecurity failures in healthcare extend beyond financial loss and data privacy concerns, as seen in Greene (2015). These attacks can directly impact patient safety, disrupt clinical operations, delay treatment, and compromise the availability and integrity of electronic health records (EHRs). The American Hospital Association (Riggi, n.d.) emphasizes that cybersecurity should be viewed not simply as an information technology issue but as a patient safety and enterprise risk management priority that must be integrated into organizational governance and risk management practices. This perspective has been reinforced by several high-profile healthcare cyber incidents. For example, the 2020 ransomware attack against Universal Health Services disrupted operations across more than 400 healthcare facilities, forced clinicians to revert to paper records, delayed patient care, and resulted in approximately $67 million in financial losses, demonstrating the operational and economic consequences of inadequate cybersecurity preparedness (Lyngaas, 2021). As healthcare organizations increasingly migrate data, applications, and clinical services to cloud environments, ensuring adequate cybersecurity readiness prior to migration is essential (Scott, 2022). Consequently, understanding how organizations can assess their technical capabilities, regulatory compliance, and workforce preparedness prior to cloud adoption has become an important area of research.

2.1 Cloud Adoption in Healthcare

Over the past decade, cloud adoption in healthcare has experienced significant growth. This trend is largely driven by the need to support electronic health record (EHR) systems, health platforms, and clinical data operations (Kuo, 2011). Research indicates that cloud technologies provide notable operational advantages, such as cost reduction, enhanced data accessibility, and improved disaster recovery capabilities (Kruse et al., 2017). However, the primary concerns revolve around security and compliance.

The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act create a complex regulatory landscape for healthcare organizations contemplating cloud migration. According to Alder (2026), staff actions are the weakest link in the cybersecurity chain. HIPAA's Security Rule mandates the implementation of administrative, physical, and technical safeguards for electronic protected health information (ePHI), while HITECH has broadened enforcement authority and escalated penalties for non-compliance (HHS, 2013). These requirements do not simply vanish when data is transferred to the cloud; they persist and must be adhered to (HHS, 2016). Consequently, organizations must assess not only whether a cloud platform can securely host ePHI but also whether they are adequately prepared to maintain compliance within that specific environment.

2.2 Existing Readiness Frameworks

Numerous cloud readiness frameworks are currently available in the industry. The Cloud Security Alliance's Cloud Controls Matrix (CCM) offers a comprehensive set of security controls tailored for cloud deployments (Cloud Security Alliance, 2021). Additionally, the NIST Cybersecurity Framework (CSF) and NIST SP 800-53 Rev. 5 provide widely accepted control baselines particularly relevant to federal and regulated sectors (NIST, 2020). Both AWS and Microsoft Azure publish compliance guidelines specifically for healthcare, aligning their services with HIPAA requirements. However, a common shortcoming among these frameworks is their primary focus on technology. They assess whether a cloud platform satisfies specific technical criteria, but overlook whether the organization migrating to the platform is adequately prepared to operate securely and maintain compliance.

Furthermore, existing readiness models often neglect the human element. In healthcare, cloud migration failures frequently arise not from technical issues but from inadequate staff training, ineffective change management, and a lack of organizational awareness regarding security responsibilities in cloud settings (Jalali & Kaiser, 2018). This trend is consistent with broader findings in healthcare cybersecurity research, which continually identify the workforce as the weakest link in the security framework (Coventry & Branley, 2018).

2.3 NIST SP 800-53 and Healthcare Security Controls

NIST Special Publication 800-53 Rev. 5 offers the most comprehensive catalog of security and privacy controls available for federal information systems, and it has been extensively adopted in the healthcare

sector as an effective mapping tool for HIPAA compliance (NIST, 2020). This publication categorizes controls into 20 families, covering essential areas such as access control, incident response, configuration management, and supply chain risk management. For healthcare organizations, the disparity between NIST SP 800-53 controls and HIPAA Security Rule requirements is considerable, positioning NIST SP 800-53 as a vital foundation for technical and compliance readiness assessments.

Additionally, CSA provides guidance on preventing ransomware attacks in healthcare clouds (Hughes, 2024). Also, AWS has released a mapping of its services to the NIST SP 800-53 controls in its Healthcare Compliance Guide, which serves as a valuable reference for organizations assessing cloud deployment options (Amazon Web Services, 2023). This mapping is an integral component of the technical domain scoring methodology utilized in the HCRF.

2.4 Bloom's Taxonomy and Workforce Readiness

Bloom's revised taxonomy, initially designed as a framework for classifying educational objectives, has also been applied to workforce readiness assessments across various professional fields (Krathwohl, 2002). This taxonomy categorizes cognitive skills into six levels, ranging from basic recall and understanding to application, analysis, evaluation, and creation. In the realm of cybersecurity education, the taxonomy has been utilized to assess whether training programs equip employees with the necessary skills for performing security-critical tasks, rather than merely exposing them to information (Clark et al., 2020).

For the HCRF, Bloom's revised taxonomy serves as the foundational structure for the staff readiness domain. Instead of merely determining whether employees have undergone training, the framework evaluates whether that training has effectively developed the cognitive abilities needed for staff to identify security risks, respond appropriately to incidents, and make informed decisions about handling ePHI in a cloud environment. This relationship between training exposure and demonstrated capability is central to the HCRF's approach to the workforce component.

DOMAIN	WEIGHT	REASON
Technical & Security	40%	Foundation for secure migration
Compliance & Risk	35%	Legal compliance & breaches
Staff	25%	Human error

Table 1: HCRF Cybersecurity Weighted Risks

According to Table 1, the technical domain received the highest weighting of 40%, underscoring the critical importance of technical security controls in protecting electronic protected health information (ePHI) within cloud environments. Compliance was assigned a weight of 35%, reflecting the significant legal and regulatory consequences associated with violations of the Health Insurance Portability and Accountability Act (HIPAA). The staff readiness domain was allocated a weight of 25%, emphasizing the role of human error in security incidents within the healthcare sector.

The grading scale is established by multiplying the score of each domain by its corresponding weight. A score below 60 is deemed a failure level, indicating that cloud migration efforts should not proceed. Scores ranging from 60 to 79 suggest some potential but warrant caution, a control review, and possible new safeguards or countermeasures. A score of 80 or above indicates that the cloud migration process is ready to proceed.

3. METHODOLOGY

This research employed a design science research (DSR) methodology to develop and demonstrate the Healthcare Cloud Readiness Framework (HCRF). Design science research is well suited for creating practical artifacts that address organizational problems while providing a structured process for evaluating their usefulness. The artifact developed in this study is the HCRF, a readiness assessment framework designed to help healthcare organizations evaluate their preparedness for secure cloud adoption before migration occurs.

The framework was constructed from an extensive review of healthcare cybersecurity literature, cloud migration guidance, HIPAA Security Rule requirements, and established cybersecurity standards, including the NIST Cybersecurity Framework (CSF) and NIST SP 800-53 security controls. These sources were synthesized into three readiness domains that consistently emerged as the primary determinants of successful healthcare cloud migration: Technical Security, Compliance and Governance, and Staff Readiness. Technical Security evaluates the maturity of security controls, infrastructure, network architecture, monitoring capabilities, and identity management. Compliance and Governance measures organizational adherence to HIPAA requirements, enterprise risk management, security policies, and regulatory oversight. Staff Readiness assesses workforce cybersecurity awareness, phishing resilience, role-based security training, and organizational security culture. The figure below illustrates this framework.

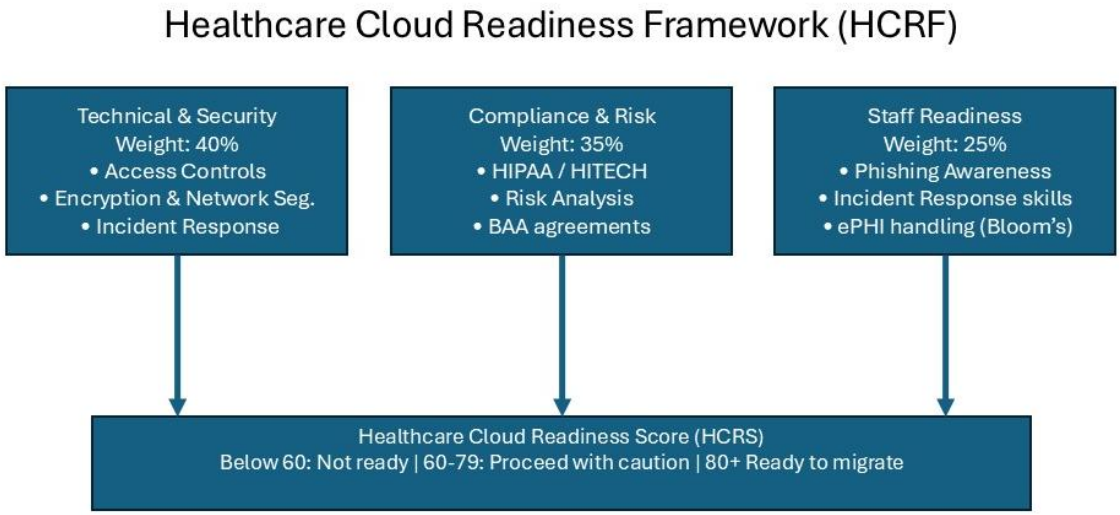

Figure 1. The Healthcare Cloud Readiness Framework (HCRF)

Each domain is scored on a 100-point scale using evidence collected during organizational assessments. Domain scores are then multiplied by the weighting factors defined in Table 1 to reflect their relative contribution to overall cloud readiness. The weighted domain scores are summed to produce the Healthcare Cloud Readiness Score (HCRS), which provides a quantitative measure of an organization's preparedness for cloud migration. Higher scores indicate greater readiness, while lower scores identify areas requiring remediation before migration should proceed.

To demonstrate the applicability of the framework, a retrospective multiple-case study approach was employed using two widely documented healthcare cyber incidents: the 2015 Anthem data breach and the 2020 Universal Health Services (UHS) ransomware attack. These cases were selected because they represent different attack vectors, organizational characteristics, and cybersecurity failures while both involving large healthcare providers with mature information technology environments.

Data for each case were collected from publicly available sources, including Office for Civil Rights (OCR) breach investigation reports, U.S. Department of Health and Human Services (HHS) enforcement and settlement documents, industry analyses, and reputable cybersecurity news reports. These sources

were analyzed to identify evidence describing each organization's cybersecurity posture immediately prior to the incident. The documented evidence was then mapped to the three HCRF domains, and domain scores were assigned based on the extent to which security controls, governance processes, and workforce preparedness aligned with the framework's assessment criteria.

The objective of the case studies was not to recreate the organizations' exact security posture, but rather to demonstrate how the HCRF can systematically identify organizational strengths, weaknesses, and readiness gaps before cloud migration. Applying a common assessment methodology across multiple healthcare organizations provides a consistent mechanism for comparing readiness levels and identifying the technical, regulatory, and workforce improvements necessary to reduce cybersecurity risk. This evaluation demonstrates the practical utility of the HCRF as a decision-support tool that healthcare organizations can use to prioritize investments, strengthen cybersecurity maturity, and improve cloud migration planning.

4. CASE STUDIES

To demonstrate the efficacy of the Healthcare Cloud Readiness Framework (HCRF), two significant data breach incidents are analyzed within the medical cybersecurity sector: the 2015 Anthem breach—the largest healthcare data breach in U.S. history, which culminated in a $16 million HIPAA settlement, and the 2020 ransomware attack on Universal Health Services (UHS), where the Ryuk ransomware disrupted operations across more than 400 institutions, leading to an estimated $67 million in costs (HHS, 2020).

4.1 Scenario 1: Anthem (2015)

The Anthem breach was predominantly instigated by a spear phishing attack that compromised system administrator credentials, enabling attackers to infiltrate Anthem's database over several weeks. The investigation by the Office for Civil Rights (OCR) revealed that Anthem neglected to conduct a comprehensive enterprise-wide risk analysis and lacked adequate procedures to identify and manage security incidents. Additionally, there were insufficient controls to prevent unauthorized access.

Utilizing the HCRF to assess Anthem's posture prior to the incident reveals critical insights. Anthem had invested heavily in technology, achieving a robust technology score of approximately 78 out of 100 due to the deployment of firewalls, access control systems, and effective data center management tools. However, deficiencies in risk analysis and detection of unauthorized access significantly detracted from its compliance score, which registered around 49. Furthermore, the effectiveness of employee training on recognizing targeted social engineering attacks was notably inadequate, resulting in a staff proficiency score of approximately 55. The aggregate HCRS score stood at around 63, indicating only a moderate level of readiness. These assessments would have highlighted compliance and employee training as key areas needing enhancement prior to any cloud migration efforts.

4.2 Scenario 2: Universal Health Services (2020)

The UHS attack was initiated by a phishing email that facilitated the download of TrickBot and subsequently led to the deployment of Ryuk ransomware on September 27, 2020. This attack incapacitated UHS facility computer systems, compelling personnel to revert to paper records, reroute emergency services, and function without access to Electronic Health Records (EHR) or test results for an extended period.

In applying the HCRF to UHS's operational profile pre-incident, a contrasting scenario emerges compared to Anthem. UHS benefited from a sizable IT organization and was generally perceived to possess strong HIPAA compliance, with a compliance rate of approximately 76. However, vulnerabilities were evident in the technical domain. Insufficient network segmentation between clinical and administrative systems permitted the lateral movement of Ryuk and the malware propagation, as the multi-stage infection chain comprising Emotet and TrickBot remained undetected until the ransomware was deployed (Trend Micro., 2026). This resulted in a technical score of around 55. Additionally, with phishing identified as the primary attack vector, staff competency registered a low score of approximately 52, aligning with findings that the breach originated from a social engineering exploit targeting typical employees. The total HCRS score for UHS was approximately 61, positioning the organization in the moderate

compliance range, while highlighting technical controls and employee capabilities as critical areas needing fortification for securing any future cloud migration.

5. CASE STUDY ANALYSIS

Table 2 shows how HCRF was applied to both case studies. Even though these organizations experienced different cyberattacks and had their own problems, the HCRF helped show what went wrong and what needed improvement before moving to the cloud. Looking at the same three areas for both organizations made it easier to see where they were prepared and where they still had work to do.

HCRF Domain	Anthem Case Study	Universal Health Services Study
Technical Security	Strong security but weak monitoring	Ransomware was spread
Compliance	Poor Risk Analysis	Good Compliance but gaps within technical aspects
Staff Readiness	Vulnerable to phishing attacks	Vulnerable to phishing attacks
Result	Moderate	Moderate

Table 2: HCRF Applied to Case Studies

To evaluate each organization, the researchers analyzed information from breach investigation reports by the Office for Civil Rights (OCR), settlement documents from the U.S. Department of Health and Human Services (HHS), and relevant news articles regarding each incident. They then assessed each of the three domains of the Healthcare Cloud Readiness Framework (HCRF), assigning a score out of 100 based on the organization's cybersecurity prior to the breach. After scoring all three domains, each score was multiplied by its corresponding weight as detailed in Table 1, and the results were summed to arrive at the final Healthcare Cloud Readiness Score (HCRS).

6. DISCUSSION

HCRF addresses a significant gap in the current landscape of cloud readiness tools. Most tools focus on whether a cloud platform can meet a set of security requirements, but they fail to assess whether an organization is truly prepared for migration. This distinction is crucial, as it explains why healthcare cloud migrations experience disproportionately high failure rates relative to available technical capabilities (Jalali & Kaiser, 2018).

The three-domain structure of HCRF is intentional. Technical readiness holds no value without proper compliance; a lack of regulatory adherence could lead to legal exposure and ultimately failure. Conversely, being compliant without the necessary technical capabilities means that while there may be policies in place, there are no controls to enforce them. Additionally, human error remains a significant contributor to security failures. The HCRF evaluates these domains independently at first to identify areas of weakness and determine how frameworks can assist.

By employing Bloom's taxonomy, HCRF distinguishes between mere knowledge and the ability to apply that knowledge effectively. For instance, an employee who can merely recall the definition of ePHI is less prepared than one who can assess whether a specific situation qualifies as a reportable breach. Ultimately, the HCRF aims to provide a more accurate measurement of an organization's overall readiness.

7. RECOMMENDATION AND FUTURE WORK

The findings of this study suggest several recommendations for healthcare organizations planning cloud migration. First, organizations should conduct a comprehensive cloud readiness assessment before initiating migration to identify technical, regulatory, and workforce gaps that could increase cybersecurity risk. Second, healthcare providers should maintain continuous compliance with HIPAA and other applicable regulatory requirements by incorporating regular risk assessments and governance reviews into their security programs. Third, cybersecurity awareness and phishing-resistance training

should become an ongoing organizational priority, as workforce readiness remains one of the most common attack vectors. Fourth, organizations should adopt established security frameworks, such as NIST SP 800-53, to guide the design, implementation, and monitoring of cloud security controls throughout the migration process. Finally, cloud readiness should be viewed as a continuous process rather than a one-time assessment, with organizations regularly reassessing their security posture as technologies, threats, and regulatory requirements evolve.

Future research should expand the evaluation of the Healthcare Cloud Readiness Framework (HCRF) by applying it to a larger and more diverse sample of healthcare organizations. Evaluating hospitals, clinics, and healthcare systems of varying sizes and operational complexities would provide additional evidence regarding the framework's generalizability and effectiveness. Further research should also investigate whether domain weightings and scoring criteria should be tailored to different organizational characteristics, recognizing that healthcare providers vary considerably in their resources, infrastructure, and cybersecurity maturity. Finally, the development of an automated HCRF assessment tool would enable healthcare organizations to calculate their Healthcare Cloud Readiness Score (HCRS), visualize readiness across assessment domains, and receive prioritized recommendations for improving cloud migration preparedness.

8.CONCLUSION

Healthcare organizations increasingly recognize the operational, financial, and clinical benefits of cloud computing; however, successful cloud adoption depends on more than simply migrating applications and data. Organizations that transition to the cloud without first evaluating their technical capabilities, regulatory preparedness, and workforce readiness risk introducing cybersecurity vulnerabilities, compliance deficiencies, and operational disruptions that could otherwise be mitigated through proactive planning. The Healthcare Cloud Readiness Framework (HCRF) addresses this challenge by providing a structured, evidence-based assessment that evaluates an organization's readiness across three interdependent domains: technical security, regulatory compliance, and staff readiness. By combining these dimensions into a single Healthcare Cloud Readiness Score (HCRS), the framework enables healthcare leaders to identify capability gaps, prioritize remediation efforts, and make more informed cloud migration decisions.

The retrospective application of the HCRF to the Anthem and Universal Health Services case studies demonstrates the framework's practical value. Although both organizations achieved similar overall readiness scores, the assessment revealed distinctly different underlying weaknesses. Anthem exhibited deficiencies in enterprise risk management and regulatory compliance despite relatively mature technical controls, whereas Universal Health Services demonstrated stronger compliance but significant shortcomings in technical security and workforce resilience. These findings illustrate that organizations with comparable levels of overall readiness may require fundamentally different remediation strategies. More importantly, they demonstrate that evaluating only a single aspect of cloud preparedness (e.g., whether technical, regulatory, or organizational) is insufficient to accurately assess cloud migration readiness.

While the HCRF is intended primarily as a pre-migration assessment tool, its utility extends throughout the cloud adoption lifecycle. Healthcare organizations can use the framework as part of a continuous governance process to periodically reassess their security posture, monitor improvements, evaluate the effectiveness of remediation efforts, and ensure ongoing compliance as cloud technologies, cybersecurity threats, and regulatory requirements evolve. As healthcare environments become increasingly dependent on hybrid and cloud-native architectures, continuous readiness assessment becomes an essential component of organizational resilience rather than a one-time migration activity.

Future research should further validate the HCRF by applying it to a larger, more diverse population of healthcare organizations across different sizes, specialties, and levels of cybersecurity maturity. Additional empirical studies should examine whether the domain weightings and scoring methodology require refinement to better reflect variations in organizational risk profiles and cloud deployment models. Future work may also explore developing an automated HCRF assessment platform that calculates the Healthcare Cloud Readiness Score (HCRS), benchmarks organizations against industry baselines, and generates prioritized recommendations to improve cloud migration readiness. Such

enhancements would strengthen the framework's practical value and support healthcare organizations in making more informed, secure, and resilient decisions about cloud adoption.

9. REFERENCES

Alder, S. (2026, January 9). Staff are the weakest link in HIPAA cybersecurity. *The HIPAA Journal.* https://www.hipaajournal.com/staff-weakest-link-hipaa-cybersecurity/

Amazon Web Services. (2023). AWS compliance: Healthcare. https://aws.amazon.com/health/healthcare-compliance/

Amod, F. (2025). Report: Human error remains a leading driver of healthcare data breaches. *Paubox.* https://www.paubox.com/blog/report-human-error-remains-a-leading-driver-of-healthcare-data-breaches

Clark, U., Stoker, G., & Vetter, R. (2020). Looking ahead to CAE-CD program changes. *Information Systems Education Journal*, 18(1), 29-39. https://isedj.org/2020-18/n1/ISEDJv18n1p29.pdf

Cloud Security Alliance. (2021). Cloud Controls Matrix (CCM) v4. https://cloudsecurityalliance.org/research/cloud-controls-matrix/

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats, and ways forward. *Maturitas*, 113, 48-52. DOI: 10.1016/j.maturitas.2018.04.008

Greene, T. (2015, February 6). Anthem hack: Personal data stolen sells for 10x the price of stolen credit card numbers. *Network World.* https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html

Hughes, J. (2024, November 14). CSA offers guidance on preventing ransomware in the healthcare cloud. *HealthTechSecurity.* https://www.techtarget.com/healthtechsecurity/news/366594940/CSA-Offers-Guidance-on-Preventing-Ransomware-in-the-Healthcare-Cloud

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research*, 20(5), e10059. DOI: 10.2196/10059

Krathwohl, D. R. (2002). A revision of Bloom's taxonomy: An overview. *Theory Into Practice*, 41(4), 212-218. https://www.tandfonline.com/doi/abs/10.1207/s15430421tip4104_2

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of Medical Systems*, 41(8), 127. https://link.springer.com/article/10.1007/s10916-017-0778-4

Kuo, M. H. (2011). Opportunities and challenges of cloud computing to improve health care services. *Journal of Medical Internet Research*, 13(3), e67. DOI: 10.2196/jmir.1867

Lyngaas, S. (2021, March 1). Universal Health Services reports $67 million in losses after apparent ransomware attack. *CyberScoop*. https://cyberscoop.com/universal-health-services-ransomware-cost-ryuk

Menachemi, N., & Collum, T. H. (2011). Benefits and drawbacks of electronic health record systems. *Risk Management and Healthcare Policy, 4*, 47–55. DOI: 10.2147/RMHP.S12985.

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53, Rev. 5). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Scott, J. (2022, March). The future of healthcare and the public cloud. *Health Tech Magazine.*

https://healthtechmagazine.net/article/2022/03/future-healthcare-public-cloud

Riggi, J. (n.d.). The importance of cybersecurity in protecting patient safety. *American Hospital Association.* https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety

Terhune, C. (2015, February 4). Anthem hack: 80 million records stolen in massive healthcare breach. *Los Angeles Times.* https://www.latimes.com/business/la-fi-anthem-hacked-20150204-story.html

Trend Micro. (n.d.). What is Ryuk ransomware? *Trend Micro.* https://www.trendmicro.com/en_us/what-is/ransomware/ryuk-ransomware.html

U.S. Department of Health and Human Services. (2013). Summary of the HIPAA security rule. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

U.S. Department of Health and Human Services. (2016). Breach portal: Notice to the Secretary of HHS breach of unsecured protected health information. https://ocrportal.hhs.gov/ocr/breach/breach_frontpage.jsf?faces-redirect=true

U.S. Department of Health and Human Services. (n.d.). Cloud computing guidance. *HHS.*

U.S. Department of Health and Human Services. (2020). Anthem Inc. pays OCR $16 million in record HIPAA settlement. *HHS.* https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/anthem/index.html

APPENDIX A

HCRF Case Study Scoring Methodology and Results

The Healthcare Cloud Readiness Framework (HCRF) was applied retrospectively to the Anthem (2015) and Universal Health Services (2020) cybersecurity incidents, using publicly available evidence. Assessment data were obtained from Office for Civil Rights (OCR) investigation reports, U.S. Department of Health and Human Services (HHS) enforcement documentation, publicly released post-incident analyses, and reputable cybersecurity reporting. Each organization was evaluated across the three HCRF domains using a 100-point scale. Domain scores reflect the documented maturity of organizational capabilities immediately prior to the cyber incident rather than the organization's post-incident improvements.

A.1 Anthem (2015)

The Anthem breach demonstrated that the organization possessed a relatively mature technical infrastructure, including enterprise firewalls, identity management capabilities, and established security operations. However, OCR determined that Anthem had not performed an adequate enterprise-wide risk analysis, lacked sufficient procedures to identify and respond to security incidents, and failed to implement appropriate controls to prevent unauthorized access to electronic protected health information (ePHI). The initial compromise resulted from a successful spear-phishing attack targeting employee credentials, indicating deficiencies in cybersecurity awareness and workforce preparedness.

HCRF Domain	Assessment Rationale	Score	Weight	Weighted Score
Technical Security	Mature security infrastructure with established perimeter defenses and access controls; however, insufficient monitoring and detection capabilities allowed attackers to remain undetected.	80	40%	32.0
Compliance & Governance	OCR identified deficiencies in enterprise risk analysis, risk management, and HIPAA Security Rule implementation, reducing overall governance maturity.	50	35%	17.5
Staff Readiness	A successful spear-phishing attack demonstrated insufficient employee awareness and resistance to targeted social engineering.	55	25%	13.8
Healthcare Cloud Readiness Score (HCRS)				63.3 (≈63)

A.2 Universal Health Services (2020)

Universal Health Services maintained a mature healthcare IT environment and generally demonstrated strong regulatory compliance. However, the organization experienced a multi-stage ransomware attack initiated via phishing, which leveraged Emotet and TrickBot malware before deploying Ryuk ransomware. The incident revealed weaknesses in technical security controls, including insufficient network segmentation, inadequate detection of lateral movement, and limited containment capabilities. As with Anthem, the initial compromise stemmed from employee interaction with a phishing email, highlighting workforce readiness as an ongoing organizational vulnerability.

HCRF Domain	Assessment Rationale	Score	Weight	Weighted Score
Technical Security	Ransomware propagation demonstrated weaknesses in network segmentation, endpoint detection, and containment capabilities despite a mature IT environment.	55	40%	22.0

Compliance & Governance	Strong HIPAA compliance program and organizational governance were evident; however, technical implementation gaps reduced overall effectiveness.	75	35%	26.3
Staff Readiness	Initial compromise through phishing indicated inadequate cybersecurity awareness and insufficient resistance to social engineering attacks.	50	25%	12.5
Healthcare Cloud Readiness Score (HCRS)				60.8 (≈61)

A.3 Comparative Analysis

Although Anthem and Universal Health Services achieved similar overall Healthcare Cloud Readiness Scores (63 and 61, respectively), the framework identified substantially different readiness profiles. Anthem's primary deficiencies were associated with governance and regulatory compliance, while Universal Health Services exhibited stronger compliance but weaker technical security controls. Both organizations demonstrated comparatively low staff readiness scores, reflecting the continued prevalence of phishing and social engineering as primary attack vectors within the healthcare sector. These findings illustrate that organizations with comparable overall readiness may require different remediation strategies before undertaking cloud migration, reinforcing the value of assessing technical, regulatory, and workforce dimensions simultaneously.