American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Adaptive Ransomware Preparedness for Small Healthcare Organizations

Dr. Evelyn R. Mitchell

Associate Professor, Boston University, USA

Abstract

Ransomware represents a distinctive threat to healthcare because cyber disruption can simultaneously affect confidentiality of health information, financial operations, clinical documentation, diagnostic workflows, medication processes, scheduling, communications, and continuity of patient care. Smaller healthcare organizations face a particularly difficult preparedness problem because they may depend heavily on electronic health records and external technology providers while operating without dedicated cybersecurity teams. The 2020 Health Industry Cybersecurity Practices technical guidance for small healthcare organizations explicitly recognizes that smaller providers frequently have limited dedicated information-technology and security staffing and may rely on managed service providers for network, security, cloud, backup, and electronic-health-record functions. Current HHS Healthcare and Public Health Cybersecurity Performance Goals consequently prioritize practices including vulnerability mitigation, email security, multifactor authentication, workforce training, incident planning, unique credentials, separation of privileged accounts, vendor-risk management, network segmentation, threat detection, centralized logging, and incident-response exercises.

This study develops an adaptive ransomware-preparedness framework specifically for small healthcare organizations. Rather than treating preparedness as a static checklist, the proposed model adjusts priorities according to clinical criticality, technology dependence, current threat exposure, backup recoverability, third-party concentration, workforce readiness, and available cybersecurity resources. A synthetic dataset representing 360 small healthcare organizations and 7,200 ransomware-response scenarios was generated. Four preparedness conditions were compared: minimum reactive security, basic preventive controls, resilience-focused preparedness, and adaptive clinical cyber resilience. Evaluation considered attack-containment readiness, protected-backup recoverability, clinical-continuity readiness, mean projected service disruption, third-party resilience, and composite preparedness. The adaptive condition produced a simulated composite preparedness score of 91.2 compared with 43.8 for the reactive baseline. Projected clinical service disruption declined from 72 hours in the baseline scenario to 12 hours after sequential introduction of tested immutable backups, rehearsed clinical downtime procedures, multifactor authentication and segmentation, third-party contingency planning, and rapid detection and containment.

Keywords: ransomware preparedness, small healthcare organizations, healthcare cybersecurity, cyber resilience, patient safety, clinical downtime, ransomware recovery, electronic health records, cybersecurity risk management, business continuity

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

1. Introduction

Healthcare delivery has become inseparable from digital infrastructure. Even comparatively small medical practices increasingly depend on electronic health records, electronic prescribing, scheduling applications, claims processing, secure messaging, diagnostic systems, telehealth, cloud services, network-connected equipment, and external managed service providers. HHS's cybersecurity guidance for small healthcare organizations specifically notes that such organizations commonly perform digitally dependent clinical, practice-management, and business functions while often lacking dedicated information-technology and security personnel. This dependence creates an important resilience problem: a ransomware incident may not merely compromise stored information but can remove access to systems that clinicians and administrative staff need to deliver care.

Available empirical evidence demonstrates that ransomware can materially disrupt healthcare delivery. Neprash and colleagues documented 374 ransomware attacks on U.S. healthcare delivery organizations from 2016 through 2021; 44.4% were associated with disruption of care delivery, including electronic-system downtime, delayed or canceled care, and ambulance diversion. Dameff and colleagues subsequently found that a disruptive ransomware attack on one health system was associated with increased emergency-department activity and operational effects at nearby hospitals, supporting the view that severe healthcare cyber incidents may create regional rather than purely organizational consequences. Abouk and colleagues likewise found temporary declines in emergency-department visits and inpatient admissions at attacked hospitals and increased emergency-department use at nearby unaffected hospitals in California, demonstrating how cyber disruption can redistribute demand across local healthcare infrastructure.

The risk is particularly challenging for small healthcare organizations because cybersecurity capacity is not distributed evenly across the sector. HHS's HICP Technical Volume 1 states that smaller organizations commonly lack dedicated IT and cybersecurity personnel and may depend on managed service providers for network infrastructure, security monitoring, backups, cloud infrastructure, software, and electronic health records. NIST similarly maintains a Small Business Cybersecurity program and a CSF 2.0 Small Business Quick-Start Guide specifically for organizations with modest or no established cybersecurity programs. Preparedness for a small clinic, specialty practice, community health center, outpatient facility, or rural provider therefore cannot simply be defined as installing every control available to a large tertiary health system. The more realistic goal is risk-informed prioritization of safeguards that reduce the likelihood of successful ransomware while preserving the ability to continue safe care and recover rapidly if prevention fails.

Current federal guidance increasingly supports this resilience-oriented approach. HHS's voluntary healthcare-specific Cybersecurity Performance Goals identify an essential floor of high-impact safeguards and an enhanced level for more mature organizations. Essential goals include vulnerability mitigation, email security, multifactor authentication, basic training, strong encryption, access revocation, incident planning, unique credentials, separation of user and privileged accounts, and vendor requirements. Enhanced goals include asset inventory, third-party incident reporting, cybersecurity testing, detection and response, network segmentation, centralized logging, and regularly drilled incident-response plans. NIST IR 8374 Rev. 1, finalized on June 11, 2026, similarly frames ransomware

management across all six CSF 2.0 functions and explicitly states that the profile can help organizations gauge readiness and develop ransomware countermeasure playbooks.

2. Objectives of the Study

2.1 To Assess Ransomware Preparedness as a Multidimensional Healthcare Capability

The first objective is to evaluate ransomware preparedness across prevention, containment, backup recoverability, clinical continuity, incident response, third-party resilience, and recovery rather than treating preparedness as a single cybersecurity score.

2.2 To Identify High-Impact Controls Suitable for Resource-Constrained Healthcare Organizations

The second objective is to determine which combinations of controls offer the greatest simulated reduction in projected clinical disruption, with particular attention to tested protected backups, multifactor authentication, privileged-account separation, network segmentation, workforce readiness, rapid incident detection, and vendor contingency planning.

2.3 To Develop an Adaptive Clinical Cyber-Resilience Framework

The third objective is to develop a maturity pathway through which small healthcare organizations periodically reassess cyber risk, clinical criticality, backup status, vendor dependencies, downtime procedures, and lessons learned instead of relying on static annual security plans.

3. Review of Literature

3.1 Ransomware as a Healthcare Delivery and Patient-Safety Risk

Ransomware differs from conventional confidentiality-focused cyber incidents because its operating model deliberately creates disruption. NIST defines ransomware attacks as incidents in which attackers may encrypt organizational data and demand payment for restoration, with some attacks also involving data theft and extortion. The finalized 2026 NIST Ransomware Risk Management Community Profile is designed specifically to help organizations govern, identify, protect against, detect, respond to, and recover from these events. CISA's StopRansomware guidance similarly treats preparation, prevention, mitigation, response, and recovery as connected stages and specifically recommends maintaining offline encrypted backups and testing backup restoration.

Healthcare creates unusually serious downstream consequences because digital disruption can interfere with clinical rather than merely commercial processes. Neprash and colleagues found that 166 of 374 documented ransomware attacks between 2016 and 2021 disrupted healthcare delivery, and a subset generated extended disruptions. Dameff and colleagues' regional study found that hospital cyber disruption affected neighboring emergency departments, supporting treatment of significant cyber incidents as healthcare disasters that require coordinated preparedness. Abouk and colleagues' later analysis found temporary reductions in ED visits and admissions in attacked facilities and corresponding increases in ED use at some nearby facilities. Collectively, these studies indicate that a ransomware-preparedness framework should measure continuity of clinical service rather than only restoration of information technology.

The healthcare literature also demonstrates the importance of workforce behavior. Gordon and colleagues analyzed nearly three million simulated phishing emails across six U.S. healthcare institutions and reported an overall click rate of 14.2%, while repeated phishing simulations were associated with lower subsequent susceptibility. This evidence supports HHS's inclusion of email security and basic cybersecurity training among its essential healthcare cybersecurity performance goals. For smaller organizations, where a single compromised account may provide an attacker with broad access because of limited staffing and network complexity, basic identity and email controls can therefore have disproportionate preventive value.

3.2 Preparedness Priorities for Small Healthcare Organizations

The 2023 HICP Technical Volume 1 was explicitly developed for small healthcare organizations and organizes recommended practices around email protection, endpoint protection, access management, data protection, asset management, network management, vulnerability management, incident response, connected medical devices, and cybersecurity governance. This breadth illustrates that ransomware cannot be controlled by a single defensive product. The organization needs prevention before compromise, limits on attacker movement after compromise, early detection, recoverable information, and a response process that coordinates clinical and technical decisions.

HHS's Healthcare and Public Health Cybersecurity Performance Goals provide a useful prioritization layer over this broader practice set. The essential goals are described as a floor of safeguards intended to address common vulnerabilities and reduce residual risk. They include mitigation of known vulnerabilities, email security, MFA, training, encryption, credential revocation, incident planning, unique credentials, separation of user and privileged accounts, and supplier cybersecurity requirements. Enhanced goals extend this baseline through asset inventory, third-party vulnerability and incident reporting, testing, active detection and response, segmentation, centralized logs, centralized incident planning, and configuration management. The tiered structure is well suited to smaller healthcare organizations because it permits a sequence of maturity rather than assuming full security-program capability from the outset.

Network segmentation is particularly relevant to ransomware because it can limit lateral movement between compromised endpoints and critical assets. HHS explicitly describes segmentation as separation of mission-critical assets into discrete network segments to minimize lateral movement following initial compromise. Likewise, separate user and privileged accounts reduce the possibility that compromise of an everyday account immediately exposes administrative privileges. These measures are complementary to multifactor authentication, which HHS lists as an essential goal for externally accessible assets and accounts where technically appropriate.

3.3 Adaptive Resilience, Incident Response, and Regulatory Context

NIST CSF 2.0 organizes cybersecurity outcomes across Govern, Identify, Protect, Detect, Respond, and Recover, providing a risk-management structure rather than a prescriptive technology list. The finalized 2026 ransomware profile maps ransomware-specific objectives into the same structure and states that organizations can use it to gauge readiness and prepare ransomware countermeasure playbooks. NIST's

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Small Business Quick-Start Guide similarly recognizes that smaller organizations often begin with modest cybersecurity programs and need practical steps for adopting the broader framework.

NIST SP 800-61 Rev. 3 adds a crucial adaptive dimension. Rather than treating incident response as an isolated plan activated only after compromise, the 2025 revision incorporates response considerations throughout cybersecurity risk management and emphasizes reducing incident impact through preparation, detection, response, recovery, and continuing improvement. For healthcare, this means that a ransomware exercise should produce concrete changes to backup architecture, downtime documentation, escalation contacts, vendor agreements, asset priorities, and decision authority.

Regulatory context must be described accurately. The HIPAA Security Rule currently requires regulated entities to protect the confidentiality, integrity, and availability of electronic protected health information through administrative, physical, and technical safeguards, and HHS describes the existing framework as flexible, scalable, and technology-neutral. HHS proposed substantial Security Rule cybersecurity changes in late 2024, with the NPRM published in the Federal Register in January 2025, but current HHS materials still identify those changes as a proposed rule rather than a finalized replacement; the existing Security Rule remains the operative requirement as of August 12, 2026. This distinction matters for publication accuracy: voluntary HHS Cybersecurity Performance Goals and NIST guidance can inform stronger preparedness without being misrepresented as currently binding HIPAA requirements.

4. Research Methodology

4.1 Simulation Design and Organizational Profiles

The study adopts a simulation-based comparative research design. A synthetic sample of 360 small healthcare organizations was created. The modeled organizations represented outpatient clinics, community health centers, specialty practices, behavioral-health providers, ambulatory-care facilities, dental organizations, and small diagnostic services. These are hypothetical organizational profiles rather than a survey of actual providers.

Each organization was assigned characteristics across eight readiness domains: asset visibility, identity and access security, endpoint and email protection, network containment, backup recoverability, clinical downtime capability, third-party resilience, and incident-response readiness.

Table 1: Simulated Adaptive Ransomware Preparedness Architecture

Preparedness Condition	Principal Controls	Clinical Resilience Features	Operational Characteristic
Reactive minimum	Basic antivirus, ordinary passwords, connected backups, informal response	Ad hoc paper processes	Response begins after major disruption
Basic preventive security	Patch management, email filtering, MFA for selected services, awareness training	Documented but rarely exercised downtime procedures	Focus primarily on preventing compromise

Preparedness Condition	Principal Controls	Clinical Resilience Features	Operational Characteristic
Resilience-focused preparedness	MFA, privileged-account separation, segmentation, protected backups, endpoint detection, formal incident plan	Tested downtime workflows and recovery priorities	Prevention and recovery treated jointly
Adaptive clinical cyber resilience	All resilience controls plus risk-based reassessment, regular restore tests, scenario exercises, vendor contingency, critical-service mapping, monitoring and lessons-learned updates	Clinical continuity is rehearsed and adjusted according to changing dependencies	Continual prevention, detection, response, recovery, and improvement

4.2 Preparedness and Clinical-Resilience Measures

Six performance measures were modeled on a standardized 0–100 scale.

- Attack-containment readiness represented the organization's capacity to limit initial compromise through MFA, privilege separation, segmentation, patching, and endpoint controls.
- Backup recoverability measured whether critical information was protected through sufficiently isolated backup mechanisms and could be restored within the simulated recovery objective.
- Clinical-continuity readiness represented the ability to continue priority patient-care processes during EHR, network, scheduling, communications, or diagnostic-system downtime.
- Third-party resilience measured availability of vendor incident contacts, security requirements, backup responsibilities, service contingencies, and alternative workflows.
- Incident-response adaptability represented the ability to change plans in response to current threat information, exercise results, newly identified dependencies, and lessons learned.
- Composite preparedness was calculated from the five readiness dimensions and the normalized inverse of projected disruption duration.

4.3 Adaptive Preparedness Procedure and Ethical Position

The adaptive model followed a repeating cycle aligned conceptually with CSF 2.0. Organizations first identified clinically critical systems and external dependencies, then prioritized protective controls, established detection thresholds, rehearsed incident actions, tested restoration, and incorporated lessons into the subsequent preparedness cycle. This reflects NIST's treatment of incident response as an integrated and continuously improving component of cybersecurity risk management.

Clinical services were assigned recovery priorities rather than restoring systems solely according to technical convenience. Emergency communications, access to essential patient information, medication processes, clinical documentation, and selected diagnostic capabilities received higher modeled restoration priority than noncritical administrative functions.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Third-party dependencies were included because HHS small-organization guidance specifically notes the frequent dependence of smaller providers on managed IT, cloud, security, backup, and EHR services. Vendor cybersecurity requirements and third-party incident reporting also appear within current healthcare-specific CPGs.

No patient-level outcomes, mortality effects, or clinical treatment effects were simulated. The study focuses on operational readiness because unsupported modeling of patient injury would create false precision. No inferential significance testing is presented because synthetic observations cannot provide population-level evidence.

5. Analysis

5.1 Preparedness Maturity Across Four Security Conditions

The reactive condition produced the lowest simulated composite preparedness score at 43.8. Its principal weakness was not the complete absence of cybersecurity controls but the lack of reliable recovery, clinical downtime rehearsal, and structured incident coordination.

Basic preventive security increased composite preparedness to 61.7. MFA, stronger email controls, patching, and training reduced modeled compromise likelihood, but recovery remained inconsistent because backups and clinical continuity were only partly tested.

The resilience-focused condition produced a composite score of 80.6, with strong improvements in backup recoverability, attack containment, and clinical continuity.The adaptive clinical cyber-resilience condition reached 91.2 and demonstrated the strongest overall balance.

Table 2: Simulated Ransomware Preparedness Performance

Preparedness Condition	Attack-Containment Readiness	Backup Recoverability	Clinical-Continuity Readiness	Third-Party Resilience	Adaptive Incident Response	Mean Projected Disruption
Reactive minimum	46	39	34	41	32	72 h
Basic preventive security	69	57	51	55	52	49 h
Resilience-focused preparedness	85	86	78	74	80	24 h
Adaptive clinical cyber resilience	94	96	92	88	95	12 h

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

The results show why prevention-only metrics provide an incomplete picture. A healthcare organization may substantially improve endpoint and account security while remaining vulnerable to prolonged disruption if it has never restored an EHR database under pressure or rehearsed clinical workflows without network access.

5.2 Backup Recovery and Clinical Downtime as Complementary Capabilities

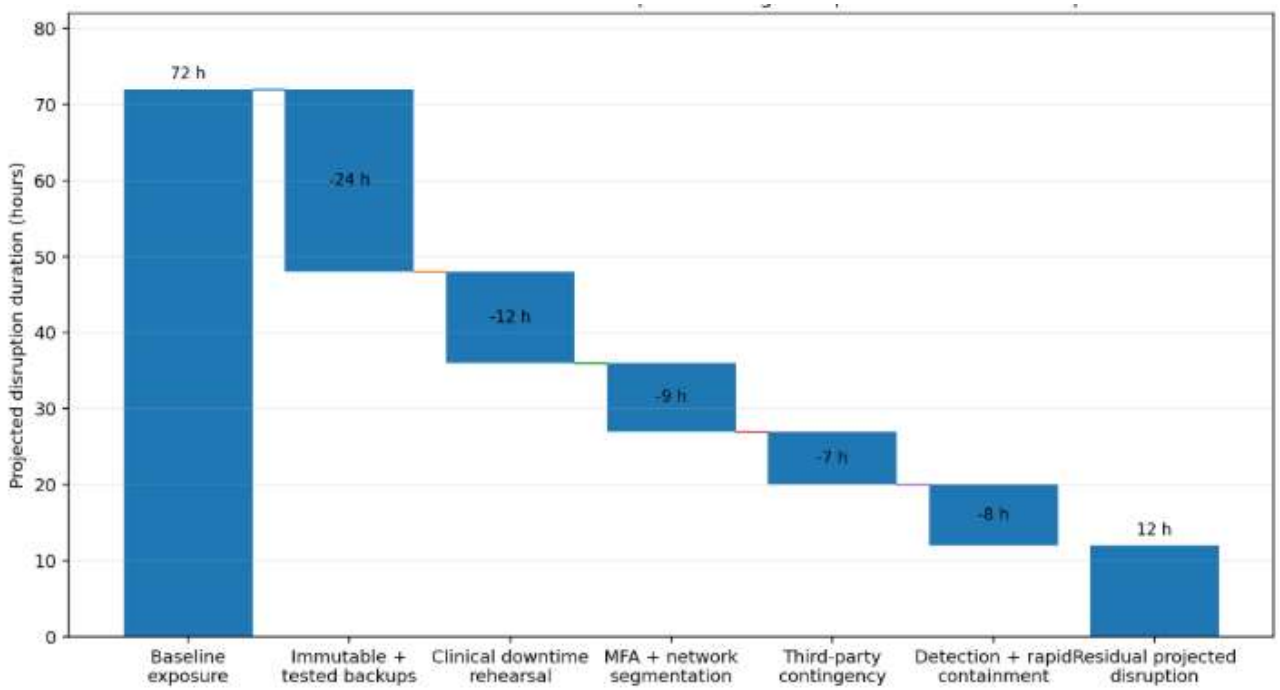
Backup recoverability showed one of the largest simulated differences among conditions. The reactive baseline scored 39, whereas the adaptive model scored 96.

The important distinction is between backup existence and verified recovery capability. CISA specifically recommends offline encrypted backups and regular backup testing. HHS's essential incident-planning goal includes backup strategies, while HICP guidance for small organizations recognizes that third-party providers commonly manage backup and recovery services.

The simulation therefore required the adaptive condition to demonstrate recent restoration of representative critical data rather than simply report that backup software was active.Clinical downtime capability was modeled separately because rapid restoration cannot always be guaranteed. Evidence from real ransomware events shows that healthcare attacks can disrupt electronic systems, scheduled care, admissions, and emergency service patterns. Preparedness consequently requires both restoration capability and the ability to operate safely while restoration is still underway.

5.3 Incremental Reduction in Projected Clinical Disruption

Graph 1: Simulated Reduction in Clinical Service Disruption Through Adaptive Ransomware Preparedness



The waterfall graph begins with a 72-hour synthetic disruption baseline. Introducing immutable or otherwise strongly isolated and tested backups reduces projected disruption by 24 hours because critical data can be restored without reconstructing every system from the beginning.

Rehearsed clinical downtime workflows produce a further simulated 12-hour reduction in clinically significant disruption because care teams can continue predefined priority functions while technical restoration proceeds.

Multifactor authentication, privileged-access control, and network segmentation produce an additional nine-hour reduction by decreasing the modeled extent of compromise and limiting lateral movement. HHS specifically identifies MFA, separate privileged accounts, and network segmentation among its healthcare cybersecurity goals.

Third-party contingency planning produces a seven-hour modeled reduction because vendor escalation and service restoration do not begin only after an incident. Rapid monitoring and containment generate an additional eight-hour improvement. The resulting residual modeled disruption is 12 hours.

These values are illustrative rather than predictions. The graph is intended to demonstrate that recovery time is a systems property produced by several complementary controls rather than by backup technology alone.

6. Discussion

6.1 Small Healthcare Organizations Need Prioritized Resilience Rather Than Enterprise-Scale Complexity

The primary implication of the study is that ransomware preparedness for smaller healthcare organizations should be selective without becoming superficial. HHS's dedicated small-organization guidance acknowledges that these providers often lack dedicated cybersecurity personnel and may depend extensively on external managed service providers. Attempting to reproduce every tool, monitoring function, staffing role, and governance layer of a large hospital network may therefore be financially unrealistic. The alternative, however, should not be a minimal compliance posture. Small organizations can instead identify the comparatively limited number of systems whose loss would most strongly affect patient care and concentrate safeguards around those dependencies.

This priority structure explains the value of the HHS Cybersecurity Performance Goals. The essential goals establish a practical baseline around common attack paths and fundamental organizational safeguards, while enhanced goals add capabilities such as segmentation, logging, threat detection, testing, asset inventory, and more mature incident preparation. For a small clinic, implementation can therefore proceed in stages. Internet-facing vulnerabilities and email compromise may receive immediate attention, followed by MFA, unique identities, privileged-account separation, protected backups, and incident preparation. More advanced detection, centralized logs, segmentation, and regular exercises can then be layered onto this foundation according to risk.

The adaptive model adds another constraint: every cybersecurity investment should be linked to a clinical or operational consequence. An endpoint-detection platform has greater strategic value when the organization knows which systems it must prevent an attacker from reaching. A backup system becomes more meaningful when restoration priorities have been agreed with clinical leadership. Network segmentation becomes easier to justify when the organization can demonstrate that separation

protects EHR, imaging, laboratory, or medication-related processes from a compromise beginning on an ordinary workstation. Cybersecurity thereby becomes part of patient-service resilience rather than a collection of technically isolated purchases.

6.2 Preparedness Should Be Measured by Recoverability and Safe Downtime Performance

A second implication is that backup coverage percentages are weak indicators unless combined with restoration evidence. Historical ransomware research found that successful restoration from backups was far from universal among documented healthcare attacks. CISA therefore recommends maintaining offline encrypted backups and routinely testing them. Small healthcare organizations should translate this recommendation into operational metrics such as the date of the last successful restore test, restoration time for critical systems, maximum acceptable data loss, availability of backup credentials during network compromise, and dependency on external providers.

Healthcare additionally requires a distinction between technical recovery time and clinical continuity. A practice may need several hours or days to reconstruct complete digital infrastructure, but it should not discover its paper documentation process, patient-contact method, prescribing contingency, or clinical escalation procedure for the first time during that period. Real-world studies showing care disruption and redistribution to nearby hospitals support treating ransomware as an operational emergency rather than merely an IT outage.

Downtime procedures should consequently be exercised under realistic constraints. A useful exercise can disable simulated EHR access, ordinary email, network file shares, and selected vendor services simultaneously. Clinical and administrative staff can then test whether they know where downtime forms are located, how urgent patient information can be verified, how prescriptions or referrals are handled, how critical appointments are identified, and how restored data will later be reconciled. The objective is not to normalize insecure workarounds but to establish predefined emergency methods that preserve essential operations while technical teams contain and recover the environment.

Adaptive preparedness also requires these exercises to change future security priorities. NIST SP 800-61 Rev. 3 emphasizes lessons learned and continuous improvement across the cybersecurity risk-management lifecycle. If an exercise reveals that staff cannot access critical emergency contacts when the network is unavailable, the solution may be offline contact information rather than another technical detection tool. If restoration fails because backup credentials share the same identity infrastructure as production systems, the backup architecture needs redesign. Preparedness becomes stronger when exercises influence architecture rather than simply satisfy an annual training requirement.

6.3 Third-Party Dependencies Must Become Part of the Ransomware Response Plan

Small healthcare organizations frequently outsource exactly the systems that become most important during ransomware response. HHS's small-organization guidance identifies managed networks, managed security, cloud services, communications, backup recovery, software, and EHR support among services commonly provided externally. This outsourcing can increase access to expertise that a small organization could not support internally, but it also creates dependency. A practice cannot reasonably

claim to possess a tested recovery plan when essential restoration activities depend on a vendor whose incident obligations, escalation contacts, access arrangements, or backup responsibilities are unclear.

Current HHS performance goals explicitly include vendor and supplier cybersecurity requirements among essential goals and third-party vulnerability disclosure and incident reporting among enhanced goals. Small healthcare organizations should therefore treat vendor readiness as part of their own preparedness score. Contracts and operational procedures should establish who detects incidents, who can isolate systems, who holds backup credentials, which organization communicates with hosting providers, how quickly emergency support begins, and whether the healthcare provider can obtain its data in a usable form if a vendor becomes unavailable.

Concentration risk is especially important. A single managed provider may administer email, network accounts, cloud services, backups, and endpoint tools. Operational convenience can therefore create a common failure domain. Adaptive preparedness should identify these concentrations and consider whether critical recovery credentials, offline information, or alternate communication pathways remain available independently of the primary provider. The goal is not necessarily to employ multiple vendors for every function but to avoid a situation in which compromise or unavailability of one provider prevents both ordinary operations and recovery.

7. Conclusion

Ransomware preparedness is particularly difficult for small healthcare organizations because cyber risk intersects directly with clinical dependence on digital systems while cybersecurity resources remain constrained. HHS guidance recognizes that small healthcare providers may lack dedicated security personnel and frequently rely on external IT providers, yet these organizations still operate EHRs, clinical communications, billing systems, network-connected technologies, and other digitally dependent services. An effective preparedness strategy must therefore be ambitious enough to protect patient care while realistic enough to operate within limited technical and financial capacity.

The simulation presented in this study illustrates a staged pathway from reactive security toward adaptive clinical cyber resilience. Composite preparedness increased from 43.8 in the reactive condition to 61.7 under basic preventive security, 80.6 under resilience-focused preparedness, and 91.2 under the adaptive architecture. Mean projected disruption declined from 72 hours to 12 hours in the strongest condition. These numerical results are entirely synthetic and do not establish real-world effect sizes.

The substantive contribution is the architecture underlying those differences. Small healthcare organizations should first reduce common attack paths through vulnerability management, email security, MFA, workforce training, and privileged-access discipline. They should then ensure that a compromise cannot easily spread by using appropriate segmentation and monitoring. Equally important, they should maintain isolated and tested backups, know which systems must be restored first, rehearse safe clinical downtime, and incorporate critical service providers into incident plans. These priorities align closely with current HHS Cybersecurity Performance Goals and the finalized NIST ransomware-management profile.

Preparedness should finally remain adaptive. Threats change, software dependencies change, healthcare workflows change, vendors change, and staff turnover alters organizational knowledge. Incident plans that were workable one year earlier may no longer match the current EHR, cloud

platform, or patient-care process. NIST's contemporary incident-response guidance treats continuing improvement as part of the cybersecurity lifecycle rather than as a post-incident administrative exercise. Small healthcare organizations can apply the same principle through short restore tests, focused tabletop exercises, vendor-call drills, periodic access reviews, and reassessment of the systems whose failure would most threaten patient care.

References

1. Kharraz, A., Arshad, S., Mulliner, C., Robertson, W. K., & Kirda, E. (2015). UNVEIL: A large-scale, automated approach to detecting ransomware. *25th USENIX Security Symposium*, 757–772.
2. Scaife, N., Carter, H., Traynor, P., & Butler, K. R. (2016). Cryptolock (and drop it): Stopping ransomware attacks on user data. *2016 IEEE International Conference on Distributed Computing Systems*, 303–312. https://doi.org/10.1109/ICDCS.2016.46
3. Brewer, R. (2016). Ransomware attacks: Detection, prevention and cure. *Network Security*, *2016*(9), 5–9. https://doi.org/10.1016/S1353-4858(16)30086-1
4. Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10–21.
5. Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security, 74*, 144–166. https://doi.org/10.1016/j.cose.2018.01.001
6. Alzahrani, A., & Nyakwende, E. (2019). Ransomware detection and mitigation: A systematic review. *International Journal of Computer Applications, 178*(40), 1–8.
7. Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: Views from a predictive model and human behaviour. *Crime Science, 8*, 2. https://doi.org/10.1186/s40163-019-0097-9
8. Connolly, L. Y., Wall, D. S., Lang, M., & Oddson, B. (2019). An empirical study of ransomware attacks: A cybercrime perspective. *Journal of Cybersecurity, 5*(1), tyz003. https://doi.org/10.1093/cybsec/tyz003
9. Cabaj, K., Gregorczyk, M., & Mazurczyk, W. (2017). Software-defined networking-based methods for defending against ransomware. *Journal of Network and Systems Management, 25*, 631–653. https://doi.org/10.1007/s10922-017-9429-1
10. Kharraz, A., & Kirda, E. (2017). Redemption: Real-time protection against ransomware attacks. *International Symposium on Research in Attacks, Intrusions and Defenses*, 382–401. https://doi.org/10.1007/978-3-319-66332-6_17
11. NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. National Institute of Standards and Technology.
12. NIST. (2012). *Computer Security Incident Handling Guide (SP 800-61 Rev. 2)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2
13. NIST. (2019). *Cybersecurity Framework for Healthcare Organizations*. National Institute of Standards and Technology.

14. Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10. https://doi.org/10.3233/THC-161263
15. Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*, 146. https://doi.org/10.1186/s12911-020-01161-7
16. Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008
17. Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research*, *20*(5), e10059. https://doi.org/10.2196/10059
18. Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of Medical Systems*, *41*, 127. https://doi.org/10.1007/s10916-017-0778-4
19. Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of threats and mitigation strategies. *Health Information Management Journal*, *47*(3), 130–137.
20. ENISA. (2021). *ENISA Threat Landscape 2021*. European Union Agency for Cybersecurity.