# BrightHealth Clinical Network - Technology Assessment Report

**Oscar Capraro, Chris Jenco, Jason Kirk, Kevin McCarthy, Anushka Tilara**

December 11, 2025

# Executive Summary

This project involved a strategic evaluation of four emerging influential technologies and their implications for Disaster Recovery (DR), Business Continuity Planning (BCP), and Crisis Management capabilities. Three of these technologies, Identity, Artificial Intelligence (AI), and Quantum Computing were predetermined as mandatory areas of analysis. To expand the scope of the assessment and further understand potential impacts on organizational resilience, the team selected Cloud Computing as the fourth technology for evaluation.

The purpose of this assessment was to understand how each technology affects an organization's ability to prepare for, withstand, and recover from disruptive events. The analysis focused on their potential to strengthen continuity operations, reduce recovery time, enhance threat detection, and improve decision-making capabilities under pressure. Key considerations included technological maturity, integration challenges, operational dependencies, and long-term implications for resilience strategies.

This evaluation highlights that each technology introduces both opportunities and risks for continuity planning. Identity technologies enhance access assurance but require strong governance. AI offers significant advantages in automation and incident response but introduces dependency and reliability concerns. Quantum computing presents future-forward and transformative impacts, especially relating to cryptography and risk modeling, but also carries substantial uncertainty. Cloud Computing offers significant advantages in scalability, availability, and streamlined recovery operations, though it introduces dependencies on third-party providers, shared responsibility considerations, and the need for strong configuration and data-protection controls.

Although each technology provides measurable value, none serve as a standalone solution. Effective integration into DR, BCP, and crisis frameworks requires policy alignment, lifecycle management, cross-platform compatibility, and sustained investment. Organizations that proactively prepare for these technological shifts will be better positioned to maintain resilience and continuity during high-impact events.

# Organizational Context

BrightHealth Clinic Network (BHCN) is a regional healthcare provider operating five community-focused clinics supported by a workforce of approximately 120 staff members, including clinicians, care coordinators, administrative personnel, and IT support staff. In addition to in-person care, the organization delivers remote medical services through its telehealth platform, enabling expanded access to patient consultations and follow-up care. These services rely on a mix of clinical, administrative, and technical systems that support daily operations and patient engagement.

As a healthcare entity, BHCN functions within a tightly regulated environment and must adhere to federal requirements including HIPAA and HITECH, which mandate strict protections for patient data, enforce robust privacy and security controls, and require timely breach notification in the event of unauthorized access. In addition, the organization must also adhere to EMTALA, which governs the timely provision of emergency medical care, reinforcing the need for reliable clinical operations and uninterrupted access to critical systems. These regulatory obligations shape the organization's operational standards, data protection requirements, and response expectations during service disruptions.

The combination of distributed clinic locations, increased dependence on telehealth technologies, and strict regulatory obligations places significant emphasis on operational resilience. Outages or disruptions can directly impact patient safety, access to care, and legal compliance, making the protection of sensitive health information, continuous availability of patient-care systems, and rapid restoration of mission-critical services essential. As a result, BHCN's Disaster Recovery, Business Continuity, and Crisis Management strategies must account for clinical continuity, secure handling of protected health information (PHI), and the ability to sustain operations across geographically dispersed clinics. These operational realities and compliance requirements establish conditions under which emerging technologies must be assessed for their potential impact on the organization's overall resilience posture.

# Technology Analysis

## Identity

Companies across multiple industries, technology-based or otherwise, rely on Identity and Access Management (IAM) for everything. In the case that IAM fails, the impact can be spread way past the company borders. Not only are employees affected, but customers may be prevented from carrying out routine tasks. Without the ability to authenticate themselves, thousands of people will be unable to access the services and technologies they need. Basic platforms that almost always required the use of identity verification include email, VPN systems, ticketing systems and way more. Not to mention, security backups are typically guarded by at least basic authentication to prevent threat actors from accessing them; meaning backups of a company's network, software and devices can be majorly compromised. Authentication outages can quickly wreak havoc, quickly becoming business continuity failures.

Identity threats directly affect disaster recovery and business continuity from multiple vectors. The most crucial one is the downfall of an Identity Provider, or IdP. Once an IdP goes down, so does the rest of its supply chain, causing outages potentially worldwide. For example, on December 3, 2025, Okta experienced an outage including LDAP connectivity issues, SMS delivery delays and overall authentication failures. This case exemplifies why IAM is crucial for DR/BC in that many employees were unable to access mission-critical systems. This outage left many customers within a particular cell stranded for many hours, but even non-global outages can deal enough damage to be severely impactful to a company's business.
In the case of multi-factor authentication (MFA) breaking, business continuity is halted by locked out users, an overflowing ticketing system, and even delays in other business processes such as incident response. If MFA breaks for higher-level security objects, domain admin accounts can be severely compromised, leaving companies unguarded.

Identity access and management should be treated as a critical infrastructure component within BrightHealth's DR/BCP. Effective mitigations for identity threats include building redundancy into identity providers. In the case an IdP goes down, there should be a secondary IdP as a failover. A second mitigation strategy could include hardening MFA and reducing single points of failure. This means using multi-channel multifactor authentication so something like an SMS

outage doesn’t block authentication. Especially for domain administrators, this should be crucial.

# Artificial Intelligence

For a healthcare company, especially one with a specific focus on telehealth, AI can prove to be a great asset. From automating customer service, to speeding up the analysis of patient scans or symptoms, AI greatly speeds up a lot of lengthy processes and cuts costs while doing so. The adoption of this technology brings many DR/BCP consequences. Since we are handling sensitive information about patients' health, we have to make sure that any AI service we use properly protects that information, and doesn’t train their models on the data we give them. Ideally the model would be hosted locally, so we have full control over the way the data is stored, and can ensure we stay HIPAA compliant.

We would also need to implement failover mechanisms for carrying out those automated tasks in a manual form if the AI service ever goes down. As with all third-party services, we must maintain the ability to operate in its absence, since we do not have control over its recovery timeline, and in the case of an outage, it may take longer for them to get back online than our patients can handle.

Another BCP consideration is around hosting. The recent AWS us-east-1 outage was a big wake up call as to how much of the internet really relies on that one service. We have to make sure that in the case of a cloud outage, our AI services are not also affected. To accomplish this, our AI services should be hosted on a different platform than the rest of our cloud infrastructure, or at least have backups on separate servers.

Finally the last big BCP concern with regards to AI is permissions. Earlier this year there was a big cyber attack targeting companies that used Drift, an AI chatbot service. Drift had been bought by Salesloft in February, and they streamlined the Drift API to work with Salesloft tokens. This opened up all the companies using Drift to a much higher level of risk, since a batch of these API tokens had been stolen by a group of cybercriminals. Since Salesloft is such a trusted company, many of the businesses who used Drift allowed it to have free reign over their documents and data, so when the attackers used those API tokens to make valid calls to a company’s instance of Drift, they could easily steal important data. To avoid an incident like

that, we should ensure that our AI only has access to the data it absolutely needs, and separate our AI services knowledge bases. Our customer service AI should never be able to access patient data, and our internal AI models that can access patient data, should not be publicly accessible.

# Quantum Computing

While quantum computing doesn't have many direct implications for healthcare in particular, it does have a big impact on cryptography and encryption which all of our digital infrastructure relies on. Modern cryptography relies heavily on difficult math problems such as discrete logarithms, or integer factorization. These problems are easy to compute, but difficult to reverse, which allows for secure encryption of data. It's not that it's impossible to reverse, just that it would take thousands of years to solve given the current processing power available to us. Quantum computing makes this null and void, since with a powerful quantum computer you could invert those equations in a reasonable time.

The main ways to prepare for this would be to ensure you migrate to post-quantup cryptological solutions. Current ones include moving away from RSA and Elliptic Curve algorithms, and towards Modern Lattice based systems which have been declared as quantum safe. Even though quantum computing is not currently available in any dangerous sense, starting a migration plan now would save a lot of headache once it does become a more prevalent threat. This would require us to audit our systems for anything that uses old encryption methods, looking for systems like encrypted file storage, or digital signatures on emails, or MFA services; then work on a migration plan, and test the new versions on a development server.

Additionally we should make a DR plan for if our encryption is broken before it is quantum safe. The crisis management team should be prepared to take down our services, and regenerate all encryption keys since even with quantum computing, breaking encryption would still be non-trivial, so a rapid switching of keys would delay attackers and could be a temporary measure to keep our communication services secure while we focus on migrating to post-quantum secure encryption.

# Cloud Computing / Cloud Infrastructure

Cloud Computing offers significant potential to enhance BHCN's Disaster Recovery (DR), Business Continuity Planning (BCP), and Crisis Management capabilities. For a small healthcare organization with limited IT staff and multiple clinic locations, cloud platforms provide robust scalability, high availability, and streamlined recovery operations. Cloud-based solutions enable geo-redundant backups, rapid failover, and centralized management, allowing clicks to continue operations even during local outages or disruptions. These capabilities directly support uninterrupted access to electronic health records (EHR), telehealth services, and patient scheduling systems.

Cloud Computing also aligns closely with healthcare compliance requirements. Cloud solutions facilitate HIPAA-compliant data storage, enforce strong access controls and PHI encryption, and provide centralized logging and monitoring. The ability to scale telehealth services quickly reduces operational strain on BHCN's IT department while ensuring secure, reliable patient care.

Additionally, cloud infrastructure integrates effectively with the other three technologies under evaluation. It complements Identity solutions through cloud-based identity and access management (IAM) and zero-trust frameworks, enhances Artificial Intelligence application with cloud-powered analytics and automation, and provides a platform for future Quantum Computing services. Together, these integrations create a cohesive technological ecosystem capable of strengthening organizational resilience and operational continuity.

# Integrated DR/BCP Risk Assessment

## Overview

BrightHealth's risk management techniques are shaped heavily by its systems reliance on each other, like cloud systems, clinical operations, telehealth services, and regulatory obligations. Due to this codependence, disruptions in operation are rarely isolated and can affect many systems in the business at once, leading to a cascading incident across multiple departments. This means that the most significant risks we can face are those capable of triggering these multi-system outages.

## External Risks

Offensive cyber related incidents are ever present and growing daily, which means one of the largest attack surfaces we face is externally. Credential compromisation, phishing, and ransomware attacks all directly threaten data security and system availability. Each of these opens up BrightHealth to widespread outages, and thus identity protection and rapid isolation are key foundations we focus on in security.

## Systems + Cloud Dependency

Cloud hosted EHR and telehealth platforms create a large dependency on constant remote availability. Clinical documentation, access to patient records, and administrative operations all rely on the absence of vendor outages, configuration errors, and authentication failures. We are able to avoid issues by implementing sufficient validated redundancy, contractual uptime guarantees, and tested failover procedures.

## Facility + Infrastructure

Continual uptime on systems is our biggest concern as a healthcare provider, so power and network failures can disrupt not only our ability to give care to our in-house patients, but also disconnect us from our telehealth customers. It will be crucial to operations to have redundancies in key systems so that we may give as constant of care as we can. We can achieve

this through backup power sources, additional connectivity routes, and multiple forms of system access, which all allow for parallel recovery.

## Financial Risks

Due to the liability we may face in downtime of billing and claims processing, and the dependence of billing systems on EHR data, disruptions or extended outages may greatly extend financial and audit exposure. It will be a priority to maintain proper synchronization and recovery methods to prevent outages as much as possible.

## Workforce + Command

Considering that the healthcare industry is largely a high-stress environment, gaps in staffing or an incoherent order of command can pose a significant risk to workplace disruption. Therefore, we will ensure a clearly defined leadership authority, succession planning, and well organized communication channels to ensure clarity and cohesion.

## Integrated Continuity Risk

Due to BrightHealth's requirement on consistent uptime, we prioritize 3 methods for mitigating risk.

1. Platform Concentration - Ensuring that critical services depend on a limited number of core systems.
2. Threat Isolation - A focus on preventing escalation of incidents across multiple departments through multiple isolation techniques.
3. Regulatory Coupling - Preventing legal and compliance exposure through rapid recovery and assurance of data accuracy.

# Strategic Roadmap

## Phase 1 (0-6 Months)

### Identity & Access

- Conduct a full IAM architecture review focusing on IdP dependencies, MFA resilience, and privileged access pathways.
- Implement a secondary identity provider to eliminate single points of authentication failure.
- Deploy multi channel MFA (i.e., push notifications, hardware tokens, voice fallback) and restrict use of SMS-only MFA.

### AI Governance

- Create policies governing AI model training, PHI handling, access controls, and requirements for a human in the loop.
- Develop a manual fallback process for tasks currently automated by AI systems.

### Quantum Preparedness

- Conduct a cryptographic inventory to identify all systems dependent on RSA/ECC algorithms.
- Prioritize high-risk systems for migration planning, including VPNs, MFA tokens, and secure messaging.

### Cloud DR Baseline Establishment

- Validate uptime SLAs and redundancy capabilities across all cloud-based EHR, telehealth, and clinical applications.
- Establish cross-region or cross-availability zone failover for EHR, scheduling, and telehealth applications.
- Perform initial failover drills to measure RTO/RPO baselines.

## Phase 2 (6-18 Months)

### Identity

- Implement continuous identity threat detection with behavioral analytics.
- Segment IAM roles for clinical, administrative, and AI-service accounts, reducing risk of

lateral movement.
- Deploy just-in-time (JIT) privileged access.

AI

- Migrate critical AI services to isolated compute environments separated from cloud hosting used by core EHR systems.
- Implement AI failover procedures and monitoring to detect bias, hallucinations, or degraded model performance.
- Deploy internal AI micro-models for clinical triage assistance using HIPAA-compliant local compute clusters.

Quantum

- Begin phased migration to NIST-approved post-quantum cryptography (PQC) for internal communications and backups.
- Test PQC compatibility in sandbox environments.

Cloud Architecture

- Implement cloud-native backup automation with immutable storage and quarterly restoration tests.
- Build a multi-cloud or hybrid failover option for telehealth services.
- Integrate centralized monitoring, logging, and incident alerting across all clinical facilities.

## Phase 3 (18-36 Months)

Identity

- Fully implement zero-trust architecture with continuous verification and network micro-segmentation.
- Complete a full annual IAM/DR simulation incorporating IdP failure scenarios.

AI

- Roll out AI-augmented incident response workflows to streamline threat detection and system recovery.
- Integrate AI-driven forecasting for demand, staffing, and potential outage patterns.

Quantum

- Complete migration of externally facing encryption systems to post-quantim algorithms.

- Finalize crisis-response procedures for pre-PQC cryptographic failure or key compromise.

### Cloud

- Operationalize cloud-native DR automation with near instantaneous failover for telehealth and scheduling systems.
- Deploy infrastructure-as-code (IaC) for rapid environment rebuilding in severe outages.
- Reduce reliance on single vendor architecture where possible.

# Executive Decisions Required

## Identity Architecture Redesign & Secondary IdP Adoption

### Decision Required

Approve funding and staffing to implement a redundant identity provider and modernize IAM architecture.

### Rationale

Identity is BHCN's largest systemic single point of failure. A second IdP is essential to prevent authentication based outages affecting clinics, telehealth, and internal operations.

### Dependencies

Vendor selection, MFA redesign, integration testing.

## AI Governance, Hosting Strategy, and PHI Compliance

### Decision Required

Selecting a hosting strategy for AI services (local compute clusters, secondary cloud environment, or hybrid hosting) and approve an organizational AI governance policy.

### Rationale

AI reliance will grow, and the organization must prevent data exposure risks, avoid vendor linked outages, and delineate which AI systems may access PHI.

### Dependencies

Compliance review, PHI data flow mapping, legal approval.

## Post-Quantum Cryptography Migration

Decision Required

Authorize the organization-wide adoption of NIST-approved PQC algorithms and dedicated funding for phased migration.

Rationale

Quantum cryptographic threats create long term exposure. Migration requires multi-year planning and testing across all operational systems.

Dependencies

Vendor capability, hardware/software compatibility, key management redesign.

## Cloud DR Modernization & Multi-Cloud/Hybrid Commitment

Decision required

Commit to a multi-cloud or hybrid architecture for telehealth and EHR failover, along with cloud-native DR automation investment.

Rationale

Cloud concentration is a strategic risk and failures at a single provider (i.e, AWS us-east-1) can disrupt continuity of care.

Dependencies

Cloud architecture redesign, subscription increases, additional staff training.

## Workforce, Training, and Crisis Leadership Structure

Decision Required

Approve the creation of structured crisis command roles, succession planning updates, and DR/BCP training programs for clinical and administrative staff.

Rationale

System resilience is limited without reliable human response capability, especially in high-stress healthcare environments.

Dependencies

HR coordination, training budget, policy reviews.

## DR/BCP Testing Frequency & Organizational Mandate

Decision Required

Mandate semi-annual full-scale DR testing and require cloud, AI, and IAM vendors to participate in coordinated continuity exercises.

Rationale

Testing validates recovery times, reveals interdependencies, and dramatically lowers the risk of multi-system outages.

Dependencies

Scheduling across clinics, vendor coordination, simulation resources.

## Funding Approval for 36-Month Resilience Program

Decision Required

Authorize a multi-year budget allocation to support the roadmap's infrastructure, compliance, and technology modernization components.

Rationale

Resilience requires a sustained investment, rather than ad-hoc fixes. Without funding commitment, BHCN will remain vulnerable to outages affecting patient care.

Dependencies

Budget cycle timing, cost-benefit analysis, competitive vendor proposals.

# Conclusion

Across the broad landscape of technologies there are to choose from, Identity Authentication, AI, Quantum Computing, and Cloud Infrastructure are the key to shaping BrightHealth's resilience against crisis. Each of these technologies have the potential to bring numerous benefits to continuous patient care and safety. However, with new technology, comes more attack surface and many more points of failure. Resilience is not just limited to adopting new technologies and assuming it will solve business continuity challenges. Instead, it depends on the careful, secure, and deliberate integration of these technologies into the organization's existing infrastructure and operational practices.

When it comes to identifying authentication services, there's a singular most immediate point-of-failure – it requires reliable redundancy and stronger multifactor resilience. Artificial intelligence has a number of operational benefits but it needs extremely strict data governance. Quantum computing currently may not have many short-term threats though it poses quite a large long-term one that BHCN should be prepared for. Cloud infrastructure expands the reaches of systems and with that, increases vendor dependence on additional third-party services.

BrightHealth's 18-36 month roadmap provides practical steps for us to modernise and strengthen security controls while also safely integrating new technology as advancements are made within the industry. BrightHealth Clinical Network must invest proactively, rather than reactively, to maintain continuity, compliance, and patient trust. With coordinated leadership and sustained disruptions, BrightHealth can ensure utmost of safe and reliable care to our patients even in the face of disaster.