TURN ADVERSITY INTO ADVANTAGE

PIVOT POINT CONSULTING
A Vaco Company

The healthcare industry continues to deal with disruption, and the recent cyberattacks on Change Healthcare has impacted the patient experience and financial operations. Attacks will continue for vulnerable organizations especially when you don't know the vulnerabilities that exist.

So how can you turn adversity into advantage? Pivot Point is here to help you work through this challenging time and re-imagine your revenue cycle management (RCM) operating model, as well as your cyber risk and security frameworks for resiliency.

We assess immediate impact and collaborate on stop-gap measures – and in parallel, we address the long-term impacts to your organization. Our experienced resources can help you leverage support mechanisms to minimize financial implications, diversify risk from concentration with third-parties, triage resourcing needs and thrive in the current environment to protect organizational value.

JOURNEY FROM REACTING TO PRESERVING ORGANIZATIONAL VALUE

REACT

- Assess immediate and long-term impact to your organization
- Prioritize recovery efforts (e.g. organization payor-mix, risk to patients, AR, etc.) based on criticality and previously conducted impact analysis results
- Determine and triage resourcing needs
- Conduct Cyber Risk Assessment and develop a prioritized roadmap
- Work with HHS and payer organizations to secure advance payments
- Develop communication strategy and engagement tools (e.g. MyChart) to proactively share solutions internally and with patients - activate executive level crisis management plan
- Identify alternative vendors and business case for automated management of lifecycle of RCM (authorization to delivery of care)

PROTECT

- Conduct review of RCM operating model and plan for transformation
- Consider diversification of third-party providers to reduce risk and conduct cyber security assessment
- Forecast continued financial impacts to ensure viability
- Develop or enhance business continuity plans to facilitate continuity of critical operations while systems are down
- Build robust cyber strategy:
  - Strategy, Governance, Risk & Compliance
  - Identity and Access Management
  - Cybersecurity Operations
  - Application Security
  - Incident Response & Risk Intelligence
  - Managed Security Services
- Build or enhance governance structure
- Implement change management to enable transformation

THRIVE

- Implement continuous improvement
- Position organization for financial resilience
- Model shifts in resourcing model
- Outline critical competencies and upskill training/career paths to enable continuous learning
- Continuous Monitoring of Third Party vendors and associated risk
- Develop roadmap to anticipate and adapt to regulatory changes
- Conduct exercises to validate continuity strategies, enabling uninterrupted services in the future