HEALTHCARE & HYBRID CLOUD: SOLUTIONS BRIEF

Delivering Patient Care Data Securely with Hybrid Cloud

Challenges:

- Cybersecurity
- HIPAA Compliance
- Patient privacy
- Interoperability of systems, networks, machines
- Accessibility of Patient records
- Monitor systems and medical devices
- Lack of skilled IT employees

Solutions:

- Hybrid Cloud portfolio encompassing multiple technical disciplines
- Role-based data and workflow access to limit exposure
- Integrated, responsive cybersecurity
- HIPAA security assessments
- Data backup and recovery
- Remote workstations

Benefits:

- Deliver Healthcare securely, with patient care top of mind
- Build trust and patient confidence
- HIPAA compliance
- Enhance patient experience
- Reduce patient frustration
- Gain visibility into your network and systems

As the healthcare industry grows in influence, it becomes more susceptible to digital attacks. High profile Healthcare organizations must respond to multiple challenges posed by customers, private insurance groups, employees, shareholders, and government compliance requirements while simultaneously maintaining robust cyber security and keeping up with technology and industry trends.

With unrelenting pressure to digitally transform, many Healthcare organizations are turning to Managed Service Providers for IT advice, expertise, and ultimately, to engage a high trust partner to share the burden of responsible data ownership.

Hybrid Cloud offers optimal flexibility to remain competitive in the industry. The key value of cloud adoption is to bridge the gap between disparate data sources and allow for greater speed, growth, and smart controls of access to clinical and business data and workflows.

While controlling operational expenses is certainly a motivating factor to digitally transform, a key driver of cloud adoption is gaining visibility and control of critical systems, networks and data to achieve exceptional patient care.

Challenges

Data is the lifeblood of any modern business, but within the Healthcare industry, the ability to collect, analyze, store, and share data securely across hospitals, labs and physicians is of primary importance for quality patient care. Data powers the business, but a data breach resulting in the loss of confidential information exposes more than PPI; it opens the door for continued attacks, hefty HIPAA fines, and the inability to recover patient confidence. Even a single cybersecurity event could result in lawsuits and financial losses that insurance policies do not cover. The long-term consequences are even worse if data backups and disaster recovery are not viable and can lead to an inability to recover patient data quickly and jump start stalled operations.

Data Integrity is a central component of Healthcare operations. Regularly testing the security controls (the access to data, breach detection, response to incidents, and monitoring the systems, networks, and environments) will determine cybersecurity risk and HIPAA compliance. Some Healthcare IT teams are so overwhelmed that they fail to properly respond even after security risks are identified.

Due to the difficulty in securing long-term, in-house, skilled IT professionals, many Healthcare facilities are trying to maintain lean teams or have outsourced IT management and cybersecurity to a Managed Service Provider. The expertise required to solve configuration puzzles between systems/networks/medical machines/environments and limit the downtime associated with upgrades, patching, and maintenance is usually more than a single Healthcare facility can afford. With fully managed solutions, you can expect systems maintenance to be proactive rather than reactive, and the associated downtime less impactful on patients and the business.

Solutions Expertise for a Disciplined Approach to Management of Data, Networks, Systems Access, and Cybersecurity

1. Assessment and Recommendations for existing security, systems, and network controls. (**Security Posture Assessment**)
2. 24/7/365 Security Monitoring – Defend against and respond to any potential infiltration of environment. (**Security Monitoring**)
3. Reduce the turmoil of running disparate systems with asset identification and uniform policy controls during mergers & acquisitions of hospitals or physician groups. (**Systems Total Care/ Endpoint Management**)
4. Balance Cloud environments based on sensitivity of data and workloads and use vendor-agnostic/best-option integration of tools and hardware into Hybrid Cloud environments for budget awareness. (**Hybrid Cloud journey**)
5. Secure data backups and data recovery with multiple locations and redundancy. (**Backup as a Service and Disaster Recovery as a Service**)
6. Remote work capabilities with contact centers and centrally managed workstations. (**Unified Communications and Desktop as a Service**)

About Us

With almost 25 years in the IT industry, TBC offers broad business management expertise as well as maintaining SOC2 Type 2 certification. With our "As a Service" model, customized to the unique needs of the Healthcare industry, organizations can rely on support through the rapidly changing demands of delivering patient care efficiently and professionally.

TBC manages technical intricacies of healthcare organizations with the rigorous standards required for compliance. Our IT teams are highly qualified to manage and support technical and security operations so you can focus on growing your business.

You can expect white glove service and true partnership to power the back-end technology needed to ensure the care and trust your
patients deserve.