CLOUD HPT

HIGH PERFORMANCE TECHNOLOGY

The State of healthcare in the UAE

Introduction

The UAE has witnessed a dramatic increase in the number of healthcare providers over the last 10 years. Today there are over 70 hospitals and 150 centers and clinics focused on primary care. With several new hospital projects due to be launched in 2017, the growth does not appear to be slowing, with many of the new hospital projects using the progress in Information Technology to deliver digital health solutions as part of their service offering to their patients.

The healthcare market here continues to evolve, the UAE government spent an estimated 2.9% of GDP on healthcare. It is also making good investments in this sector in order to attract GCC nationals and expatriates who have traditionally traveled abroad for serious medical care. This has lead to an explosion of Medical Tourism (See infographic from below).

Expected growth in Dubai medical tourism

2009 -	2012 -	2016 -	2020 -
12,000 tourists	**107,000** tourists	15% increase **107,000** tourists	20% increase **500,000** tourists
	AED 652.7 million in revenue	**AED 1.1** billion in revenue	**AED 2.6** billion in revenue

"By **2020** Dubai's private health-care sector will need approximately **1,500** new hospital beds translating into an estimated investment of **US$ 1.5 billion**."

Colliers International

Dubai Healthcare sector forecasts for 2020

3.48 million
people estimated in Dubai

3,000
more doctors required

1,500
new hospital beds required

US$ 1.5 billion
investment required

Dubai has developed Dubai Healthcare City (DHCC), a free zone that offers international advanced health providers ranges from hospitals, specialized centers and clinics as well as an academic medical training center. Moreover, Abu Dhabi has been able to affiliate its public hospitals with renowned international healthcare provides. The establishment of Abu Dhabi Cleveland Clinic is considered as a milestone in the healthcare development in the UAE. Additionally, we should not forget the significant role of the private sector healthcare investment in the growth and development of the country's healthcare sector.

UAE healthcare market to grow 12.7% to Dh71.56bn by 2020: Alpen Capital

The push towards Digital Health

While it is clear health care is undergoing a huge boom in terms of growth and investment in the UAE, it cannot be overstated that with so many players entering the market competition between providers is set to increase. In order to be competitive and in order to stay ahead of the competition, many providers are looking to technology and innovation as a key focus.

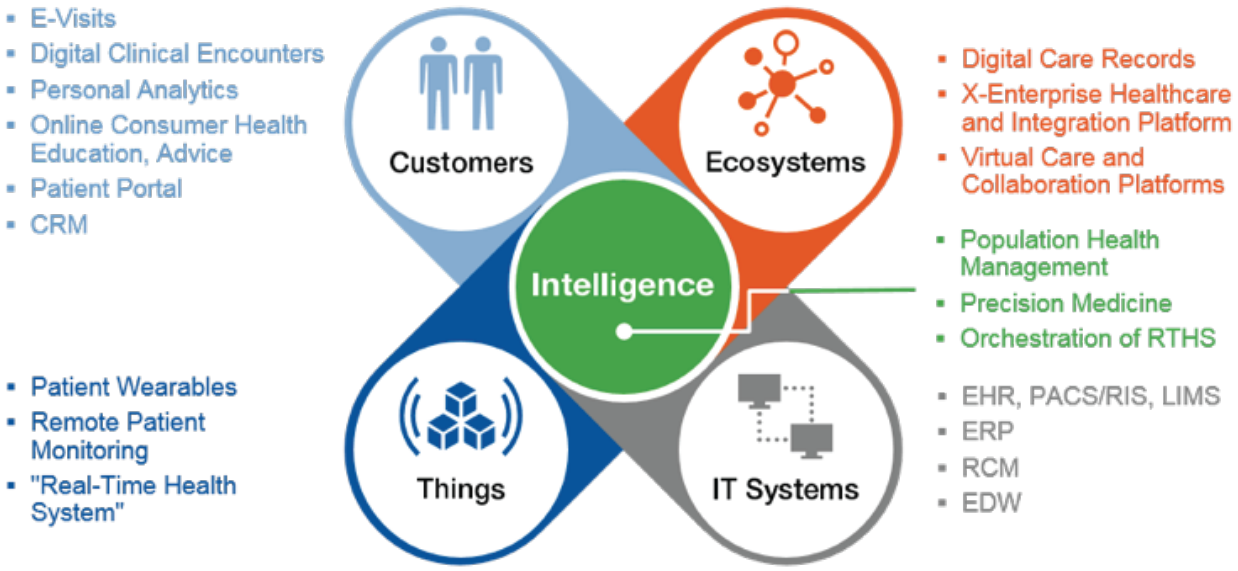
Analysis from Gartner in 2016 states that
"The disruption of digital is impacting all industries. Healthcare is no exception, and there is both uncertainty and opportunity for innovation. Clinical and business workflows will be re-engineered to put the patient at the center by connecting core systems with other platforms for IoT (both consumer- and HDO-managed), customer engagement (e.g., CRM, patient portals and apps) and broader connectivity to other ecosystems. At the center is the demand for richer real-time data to drive performance on quality, cost and experience."

The trend towards these new initiatives is being driven by the emergence of service providers who can supply either primary services; or supplementary services to free up the healthcare providers own resources to focus on delivering new projects.

Gartner predicts the trends for the coming years as
"This presents real opportunities for CIOs to identify the innovations of today that will be mainstream tomorrow and prepare for this change. We predict that within three to five years:

- EHRs (Electronic Health Records) will not be sufficient in meeting the digital business needs of the healthcare delivery organization (HDO) and a new platform will be needed.
- Virtual health assistants will be part of the virtual care strategy and a best practice for managing patients with chronic conditions.
- U.S. ERP will be entering a generational system replacement period. Cloud-based postmodern systems will be mainstream in five years, and the market share leaderboard will change dramatically.
- We also predict that biometrics will replace current forms of patient identification (such as bar coding and wrist bands), and genomics will be used for prescription writing."

The 5 key elements in technology for Patient Care



It is clear from the above that demands on healthcare IT environments are growing and will continue to grow at a rapid rate. Systems support the delivery of patient care, preserve reputation, and underpin the business resiliency of the entire enterprise. With technology, customer expectations, and the competitive marketplace changing at light speed, systems that are functioning today will likely hold providers back tomorrow.

So how do you take the first step and continued steps on the road towards your digital health strategy? The first step is to ensure you have adopted the best practices for management and delivery of your current IT environment so to ensure it is fit for purpose, scalable, resilient and extremely agile.

4 IT strategies for building a platform to deliver a digital health vision on:

1. Outsourcing all non-application based IT functions to achieve an SLA driven model for management of infrastructure with C level reporting in place.
2. Leveraging the Cloud for cost and availability benefits to deliver applications faster to more users and more customers than ever before.
3. Ensuring Business Continuity so that issues with production will not impact patient care or cause reputational damage.
4. Implementing a Total Data Protection strategy to protect data from theft as well as loss.

Let's review in greater depth how these IT strategies can help make your IT environment is ready for the challenges ahead.

Strategy 1: Outsourcing

Outsourcing Helpdesk Operations

Healthcare providers rely on smooth running of helpdesk services to provide round the clock support for users as they operate 24 hours a day, seven days a week. However often their end user helpdesk function operates normal office working hours or extended hours at best. The cost of manning the desk day and night is prohibitive, yet the requirement persists. Additionally the number of staff is often too few to cater with high concurrent demands leading to some support cases being open for days and weeks at a time.

We also observed that customers have different standards in delivery of helpdesk services. Some are quite highly structured following ITIL process and using modern helpdesk systems and perform problem management, effective change control and service review along with standard support incident management services. However the majority of IT service desks we encounter are managed ad-hoc, with little to no focus on ITIL process with little information being reported back to the business. Therefore it is hard for the business to ascertain the effectiveness of the service being provided internally.

Critically though, key members of IT staff are usually swamped with end user and network operational support. These are the very same staff members that could be adding value by working on projects that drive the Digital Health Strategy.

Outsourced Helpdesks can provide the following benefits:

- 24/7 cover including public holidays by phone, email or portal.
- Prioritization and assignment of tickets based on SLA and ticket severity (not just who shouts loudest)
- Root cause analysis
- Service level driven activity on a ticket from creation to closure, including time based escalation dependent on severity
- Considerably better response time and effectiveness of ticket handling
- Communication between the end-user and the technician
- In-depth monthly reporting
- Removal of HR cost and sickness cover for internal staff
- Coverage regionally and even world wide

How can BIOS Assist you with an outsourced helpdesk?

Our healthcare helpdesk offering is called BIOS Assist. In the example of Now Health, they had severe issues with helpdesk service being provided internally. Tickets were being reported closed without being resolved. Engineers would take up a whole day to fix individual issues, neglecting other issues and users for hours, sometimes days at a time. When the team members took annual leave there was not enough cover for peak demand and any out of hour's issues were left unresolved until the following morning.

BIOS Assist took the budget they were currently paying for ad-hoc services onsite and transformed it into a service where users are responded to in real time by highly trained service desk engineers 24 hours a day. The business reported that tickets are being closed 50% faster on average and the waiting time for response to issues has been reduced by 70%. 24/7 coverage also helped isolate users machines that were infected with ransomware before it was able to spread through the network and bring down the whole business.

The BIOS Assured NOC in Dubai.

By reviewing the trends within the support tickets on a quarterly basis with the customer, we were able to recommend process improvements such as removing admin privileges and updating group policy settings to reduce tickets for users, resulting in a 30% drop in the average monthly ticket count after year 1.

Outsourcing the Network Operation Center

All hospitals rely on a Hospital Information System (HIS) to run their operations. Typically these are large costly investments in software licenses and hardware to run them. Accordingly many other functions within the hospital require expensive bespoke applications and hardware, for example PACS, radiology, lab management, data warehousing, patient services and business intelligence to name a few. Coupled with a large sprawling network and security devices, this becomes challenging to effectively manage internally. Due to the scale and complexity of the IT environment, the healthcare provider often needs big teams in IT at great cost to manage the whole.

Teams are often made up of an IT Manager, Helpdesk Manager, Infrastructure Manager, Application lead, Development teams, Database admins, Infrastructure team, Helpdesk team and Project coordinators. Often most of the intellectual property is held in the application and database functions as they are at the internal customer facing side of IT and help shape the way IT is consumed by the users.

Infrastructure and security management, however, is often delivered as a two tier model. The base tier is the day to day administration tasks, often serviced by the internal staff with more complex changes being outsourced to professional service providers either on a monthly retainer or one time charge. This model exists because it is very difficult for the healthcare providers to source and retain engineers with the capabilities to manage their infrastructure effectively. Highly skilled resources in networking, security and datacenter technologies demand large salaries making them cost prohibitive for the healthcare provider. However, given as we have previously stated, large investments go into purchasing this infrastructure, there is an obvious disconnect which leads to healthcare providers not being able to realize the value of their investments.

Through years of providing reactive support to our customers, we observed the following issues with in house network operations:

- Critical server patches not applied, causing support and security issues
- Backups failing and not being noticed
- Capacity management being neglected leading to downtime
- Software, IOS and firmware updates not undertaken leading to performance issues and downtime
- No formal change control process, ad-hoc changes made frequently without thought of knock on effect, leading to service unavailability
- Network monitoring not in place or not installed correctly meaning a lack of visibility of issues
- Complex issues not dealt with until they are outsourced
- Significant downtime and non-availability of services that was preventable

How can BIOS help you deliver with Assured Network Operations?
Through years of working closely with many health care providers in the GCC, we have established and tested a framework of proactive maintenance, system monitoring and 24/7 coverage for priority one cases. By leveraging industry leading tools to automate essential tasks and controls we are ale to ensure that preventative maintenance is done in a timely and professional manner. We call this service **BIOS Assured** and it is the mainstay of our business, supporting both on premise and on cloud critical IT infrastructure.

Outcomes Assured delivers include:

- 24/7 response to critical issues and round the clock network monitoring meant on average a 50% reduction in the amount of unscheduled downtime
- Access for the customer to highly skilled engineers means a consultative approach to improving the performance, availability and reliability of the environment over time
- We help customers reduce cost, by managing capacity, monitoring performance and advising on how to optimize the return from their investment
- We provide escalation cover in times of crisis, ensuring that priority one cases are dealt with immediately to ensure operations are not unduly affected
- We resolve persistent issues and remove bad operating practices
- Provide an SLA driven model, increasing visibility of the effectiveness of IT to the business

How do we do it?
We have a framework consisting of 5 phases, Assess, On-Board, Manage, Protect and Optimize.

Assess – an in-depth assessment using tools to gather configuration information about the environment.

On-Board – roll out of the monitoring tools, configuration of patching, backup, configuration management, remote support functions and documenting the particulars of the environment.

Manage - We use various tools to take an in-depth look at networking, virtualization, storage, domain, servers, backup, applications and security devices. The information gathered will put a spotlight on the collective misconfiguration, incorrect settings and parameters that cause components of your network to underperform or have recurring issues. This allows us to prioritize the problems and address issues faster, having more visibility on the actions to aid quicker resolution. After completion of this phase the general operations of the environment should be running smoothly with the disruptions to service you were facing removed from further occurrence.

Protect - Protected phase focuses specifically on your security settings. We ensure that all critical patches and updates are applied to reduce the vulnerability footprint of your environment.

Optimized - Only once the environment is stable, well managed and protected can we shift the focus to enhancing what you have. The optimize phase will deconstruct previous mistakes and allow you to realize the full benefit of your investment.

In the case of Dr Suliman Habib, they opened a new high-end primary care hospital in Dubai Healthcare City in 2015. To enable better working practices for doctors and nurses they rolled out a fully virtualized environment including the desktops. The infrastructure was rolled out by the chosen contractor from the parent company from Saudi Arabia and BIOS delivered the virtualization element. Immediately after roll out it was apparent that the local team did not have any of the requisite skills to manage the environment on an ongoing basis. We delivered BIOS Assured and immediately began to observe configuration issues with the environment. During a 6 month period of assessment, monitoring, reconfiguration, observation and approval we were able to resolve all of the pre-existing technical issues. From being able to rely on BIOS Assured, the customer was able to focus their efforts on their end users and helping with adoption of technologies, many of which were new to the user base thus, providing a smooth transition into digital health ready environment.

Strategy 2: Leveraging the Cloud

“It's time for cloud service providers to be considered trusted partners to healthcare delivery organizations.” Gartner 2016

CIOs are under pressure to adopt cloud services for reasons other than cost savings, such as the desire for greater security, availability and performance, delivery to multiple sites and improving compliance. When able, the trend has been for healthcare IT leadership to take measured steps toward the adoption of cloud-based ‘as a’ services.

In the past CIOs have stepped lightly into the world of cloud-based IT services for both infrastructure and application solutions, and with good reason. There has been a general reluctance to embrace cloud offerings, particularly for protected health information (PHI), due to concerns over Health Insurance Portability and Accountability Act (HIPAA) readiness and security.

This reluctance is now unfounded. In almost all cases, cloud service providers (CSPs) have more robust and comprehensive security practices and security talent than are available to most HDO (Health Delivery Officers) and their IT departments. Cloud services have matured, as have the practices for cloud-using organizations, and the time has come for CIOs to recognize cloud service providers' strengths and consider cloud-based hosting services as a viable regulation-acceptable IT service delivery model.

A study of just under 1,600 PHI (Protected Healthcare Information) breaches impacting 500 or more individuals were tracked by the U.S. Department of Health and Human Services over the last five years. Two hundred of those were hacking events, and out of those, only one Cloud Service Provider (CSP) was identified (It was not for a PHI disclosure, but because there was a possibility it had allowed a virus injection attack on systems that contained PHI). All of the other registered breaches were due to security failures at the Healthcare provider. This should no longer be considered a surprise. From a technical and operational perspective, CSPs are executing at a very high performance level. CSP’s have invested in top-tier infrastructure housed in state-of-the-art data center facilities and managed by the experienced engineers on a 24/7 basis.

An excerpt taken from Gartner’s Healthcare review in 2016 states that:

- “Healthcare providers' rigorous regulatory requirements are driving cloud service providers (CSPs) toward risk and security standardization.
- Cloud service providers' offerings, in most cases, are more secure than healthcare providers' internal IT services.
- Achieving value from cloud services requires healthcare providers to incorporate cloud computing strategy within their larger IT strategic planning.
- By 2018, the number of healthcare providers using disaster recovery as a service (DRaaS) will exceed the number using traditional, syndicated recovery services.”

So does this mean you need to move all your applications immediately to the cloud?

The short answer is no, what we recommend is that you engage BIOS on a needs analysis first. We can assess the overall suitability of your current environment and recommend a strategy for you moving forwards. This may lead to a roadmap for cloud migration, or a hybrid cloud approach. Some key indicators you should engage with us on this are:

A) Your core infrastructure was purchased more than 3 years ago and no significant updates have been done in that time.

B) You have had a security breach or are worried you might be susceptible to one.

C) You're considering application upgrade or roll out of a new application

D) You're facing performance or reliability issues

What are your Cloud Options?

Most countries and regions are moving towards strict data sovereignty laws. Simply put they do not want Personal information and Identify data being stored outside of the country. This precludes the two typical Hyper Scale Cloud Providers.

Realizing our clients needed an in-country cloud, we at BIOS have built an ISO27001 compliant cloud instance in Dubai and Abu Dhabi that can be audited against HIPPA. It is built on CISCO's Secure and 'High Performance Technology' and as such named Cloud High Performance Technology or CloudHPT for short. CloudHPT is the regions only Cisco Powered Cloud, established in 2013, we have over 2,000 servers and 1PB of customer data. The solution is fully managed and includes an advanced security analytics platform.

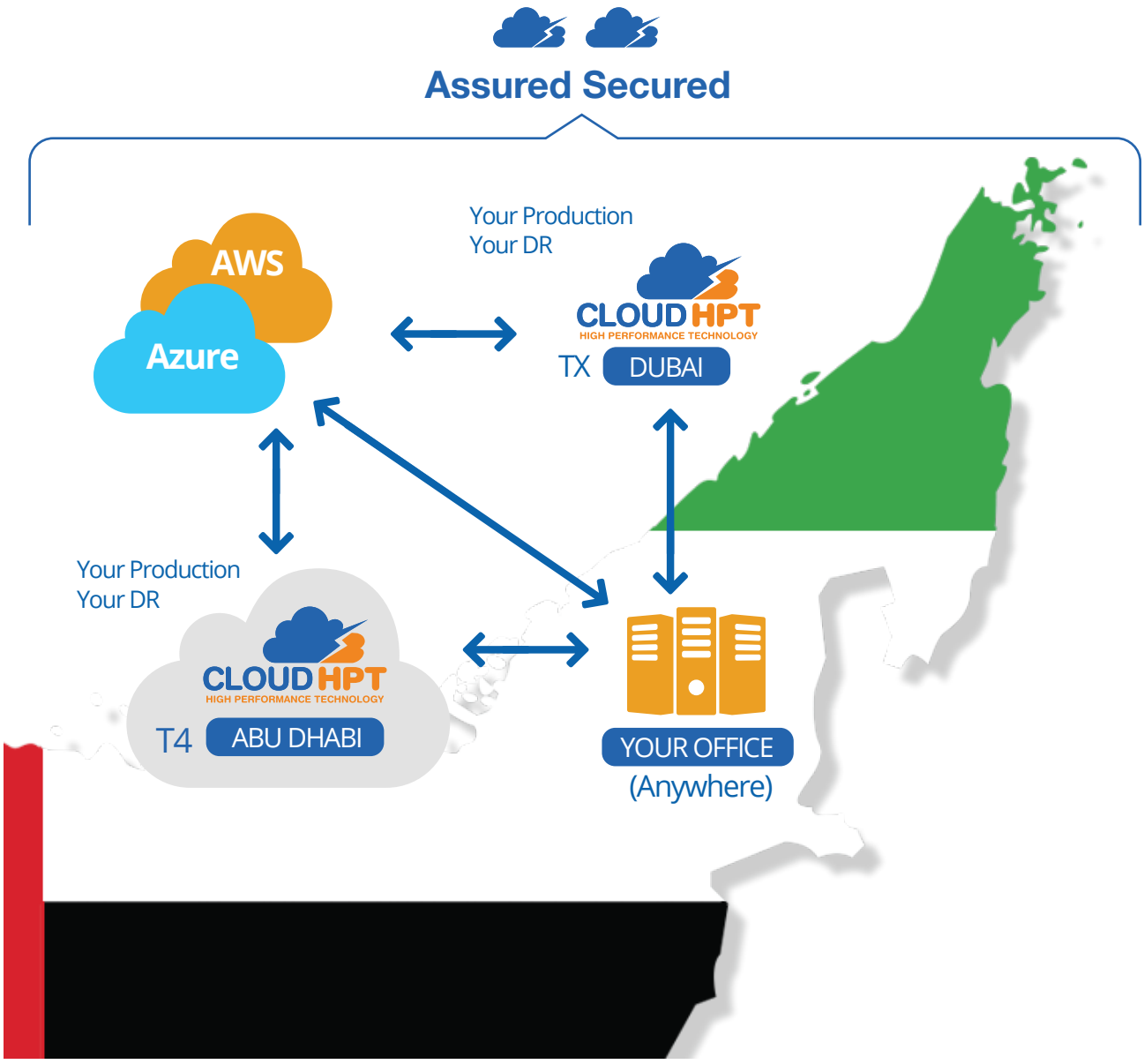
Who is using cloud in the UAE?

One example is Avivo Group who have 2 Hospitals, 10+ clinics and 2 diagnostics centers in the UAE. When they purchased a new HIS system they wanted a central repository of all patient record data and hospital information for better reporting and analysis. This required it would be centrally hosted and delivered to all locations. When they compared the options of moving to CloudHPT and procuring servers themselves and co-locating in a data center they found the following:

- The cloud option came with full managed services, whereas an in-house solution would require hiring staff or a 3rd party contract
- The cost of bandwidth with for cloud (operating out of Equinix) was 70% cheaper than from the local providers
- The Cloud solution came with enterprise class security such as firewalls, IPS, anti-malware and SIEM backed by 24/7 Security Operations Center in Dubai, which they could not provide by doing the same in-house

- The availability of the cloud option was 99.99% and a response time of under 15 minutes for any critical issues, which they could not achieve themselves
- The Total Cost of Ownership of moving to the cloud was 45% less per annum than building and maintaining their own solution

Today CloudHPT hosts the HIS for Avivo Group and many other Healthcare providers using a hybrid IT approach.



Strategy 3: Ensuring Business Continuity

Healthcare IT involves a complex hybrid environment. You may be 50, 60, or 70 percent virtualized, but you also have mission-critical legacy systems. Any outage of the production environment can impact patient care and inflict reputational damage. One this is for sure, any Healthcare provider planning on building a digital platform needs to ensure it is built on a robust foundation.

Healthcare providers daily operations are likely supported by many software vendors. With this a vast number of "moving parts," it's vital, therefore, to take an end-to-end view of your infrastructure, examining such aspects as:

- Application tiering. What are the interdependencies that exist between applications, and how does that impact how applications need to be tiered for recovery purposes?
- Recovery time objectives (RTOs) and recovery point objectives (RPOs). You may have a 4-hour RTO or RPO for a certain application, but what if your application vendor can't deliver? How would that impact patient care or your reputation?
- Testing. How comprehensive have your disaster recovery tests and exercises been? How frequent? How successful?

For example, if you have an inpatient electronic medical record (EMR)you would correctly assign this as a Tier 1 applications with 4-hour RTOs. But you also have to factor in that this application is fed by hundreds of other applications – some of which are critical for patient care. Unless the critical secondary systems are up and running, it doesn't matter if your ERM has a functional 4-hour RTO – the data it contains will be out of date, which impacts patient care and puts lifes at risk.

Testing is the best way to determine if you have identified all interdependencies and assigned tiers correctly. But the tests have to be comprehensive. They need to test the People (Who will declare a disaster? Who will perform the DR, who is responsible to checking data consistency? etc) and the Process (What is the escalation plan, Who will inform customer service, where will the teams meet, as well and not just the technology.)

As you seek to innovate patient care and strengthen business resiliency, it's good to examine your healthcare IT environment and inquire where complexity can be reduced or application agility enhanced. Virtualizing as much as you can and replacing legacy equipment can be curtail steps in a winning strategy here.

Making sure you have an **Assured Recovery Services** in place.

One option would be to work with us. We have built a end to end DRaaS service that leverages our Assured Managed Service and In country Cloud CloudHPT. It is called Assured Recovery Service (ARS).

For health care providers we provide a fully managed platform to protect critical data from loss and ensure availability. The solution protects their businesses, helps with compliance and is much more cost effective then in-house alternatives. Usual Outcomes of ARS include:

- A testable and auditable Disaster Recovery solution that will be fully documented.
- A Return to Operations time of under 30 minutes, minimizing business impact in the event of a disaster.
- Near zero recovery point objective (RPO) means minimal data loss for your business.
- Fully managed SLA to reduce your operational costs.
- Monitoring of production environment to detect downtime
- Data stored in the best DCs in the UAE
- 24x7 support from our state of the art NOC in Dubai.
- Can be quickly implemented – usually less than two weeks.
- Doesn't require any additional hardware.
- Will improve support for your IT systems, particularly in time of crisis.

Who is using DRaaS in the UAE?

Mediclinic approached BIOS to provide an offsite backup solution for City Hospital as they have around 50TB of data and 120 servers at this location. We discussed with them the requirements of the solution and it appeared they were opting for a cold site DR solution. We then met with all the key stake holders and discussed the pro's and con's of DRaaS. As they were not aware such an option was available for a cost that was 75% cheaper than the estimated cost to build their own DR site, they invited us to do a full investigation of how to deliver DRaaS. The customer had completely physical server infrastructure, including key systems such as HIS, PACS and Radiology. We spoke to all application vendors and got approval to virtualize the front end servers, this meant speaking to GE, Philips, Xerox and more. When we got approval we proposed the customer to contract us to build a VMware cluster so we can provide the best SLA around cloud replication and recovery. Within 2 months we had virtualized the whole environment and then we got to work on the DR.

DR was done in two phases, non-critical services first, then testing, then critical services. Within 4 weeks we had rolled out the full DR solution and tested failover. Approximately 2 months after go live City hospital had to fail over their HIS system to CloudHPT for 1 week due to a major corruption that required a system rebuild. It was estimated they would have lost 500,000 AED due to this outage if our service had not been in place. Since then Mediclinic have also rolled out the service to Welcare Hospital making this the biggest DRaaS environment for a Healthcare provider in the country.

Strategy 4: Total Data Protection

There are few types of data more important, sensitive and private then Electronic Healthcare Records. As such the loss or theft of any of this data could lead to devastating outcomes for the patient and the healthcare provider. This is why so much compliance has sprung up around healthcare with major financial penalties for those who fail in this regard.

When Data loss does happen, typically 75% is due to issues from within the organization and 25% from malicious activity. The latter is likely to grow as ransomware becomes more and more of a threat in 2017. In any case, the odds of a healthcare provider surviving a major data loss or theft is not a given. Aside from the devastating reputational damage at the time, litigation is the likely outcome.

How traditional approaches to data protection are not sufficient in the digital age.

As stated above, data loss occurs in two main ways, namely:

1) Loss of Data from internal activities
2) Loss or theft of data form malicious activities

The traditional approach would be:

1) Use tape to protect against loss from internal activities
2) Use Firewalls and IP (Intrusion Prevention Systems) and Anti-virus and Anti-malware to protect against theft and loss from malicious activates.

The problems Tape backups:

You don't keep music on a tape keep patient data there

- Your data is everywhere, on your storage, servers, hand held devices, laptops and in the cloud.
- Spiraling cost of maintaining tapes over time.
- Annual processes cannot keep up with modern day IT demands.
- The need to restore tapes every few years and re-back them up to the latest media so they can be read in future
- The need to maintain legacy devices to read archive tapes
- The fact that the media is sensitive to dust, heat, moisture and vibration all of which can render the tapes unreadable
- And that a lot of tapes are sent offsite without the data restore function being checked first
- Backups fail often
- Backups takes days/weeks to restore if at all.

The problems with using security devices such as Firewalls and IPS to protect against malicious activity:

- They are configured by humans and humans make mistakes and leave gaps
- Usually they are a standalone collection of devices not integrated
- The amount of data they produce is enormous and difficult for anyone to comprehend
- Security is rarely tested
- Hackers and Viruses come up with new Zero day threats continuously.

How does 'Total Data Protection' address these issues?

First, we address the threat of losing data with an automated in country cloud backup solution. This solution can backup data from storage, servers, mobile devices, laptops and other cloud instances and provides the following advantages over traditional backup:

- Ability to store data remotely on disk for faster recovery
- More cost-effective than in-house solutions and processes
- Predictable costs (i.e. simpler budgeting)
- Improved support for remote office/branch office locations
- Improved service levels
- Ability to bulk restore to disk direct from the datacenter, rather than download from the internet

Secondly, we address the threat of malicious activity using a fame work called BIOS Secured. BIOS secured consists of:

- Regular external scans of your environment designed to show what a hacker can see and highlight any weaknesses
- The implementation of SIEM as a Service (Security Incident & Event monitoring) which gathers information from your security devices and IT environment including but not limited to servers, storage, mobile devices, other cloud instances and reports back suspicious and malicious activity to our 24x7 SOC.
- A 24x7 SOC based in the UAE that can detect and remediate against malicious activity in real time

It is by combining our CloudHPT BaaS and our BIOS Secured framework that we can give our customers Total Data Protection.

For Example:
Anglo Arabian Health Care use CloudHPT backup as a Service along with our IaaS platform to provide total protection services for their business. Anglo Arabian run their critical workloads are on CloudHPT IaaS and they are protected by BIOS secured. They now have peace of mind that 100% of their business is being protected, using the right service level and technology to fit the application profile, thus saving money and using the cloud intelligently to fit their business needs.