Services

2020 Vision of

The Road Ahead

technology just around the corner

The 2020 Vision of the Road Ahead newsletter presents a series of practical, strategic, and forward-looking viewpoints on healthcare technology:

"If we do a smart job of investing in healthcare modernization — let's just say, as an example, helping local hospitals and providers set up electronic billing and electronic medical record, that experts across the spectrum consider to be an important step toward a more efficient healthcare system."

President Obama
February 2009

A perspective on Dell Trusted Healthcare Cloud and why creating it is like the moon landing.

In 1961, President Kennedy's national goal was to land a man on the moon. In his May talk to a joint session of Congress, he stated, "I believe that this nation should commit itself to achieving this goal, before this decade is out, of landing a man on the moon and returning him safely to earth."

At the time, people thought manned space flight was impossible, or close to it. At the time of his speech only two people had been to space in a limited way and no one at that time had completed a single revolution around the earth. (John Glenn did this a few years later in the Mercury program.)

His trusted advisors told him the technology was decades away; it would cost hundreds if not thousands of lives, and, if the astronauts did make it to the moon, viruses in the lunar soil they would bring back would wipe out all life on earth.

While he understood the concerns, he also knew the value of a shared "generational" goal. In a few years, over two million people were actively involved in solving all the problems, developing the technology, and finding the first brave astronauts to complete this goal. In July 1969, Neil Armstrong and Buzz Aldrin did indeed stand on the moon.

Similarly, President Obama has set an equally "impossible" national goal: for everyone to have an Electronic Healthcare Record (EHR) by 2014. The EHR supplies the caregiver with the patient's most current and correct medical information and includes safety programs to prevent inadvertent medical errors. Physicians, nurses, and others can provide the highest quality care possible, because they can make decisions using the evidence-based medical informatics in the EHR.

The challenge is to provide a secure data file in a set format that any healthcare provider can access when needed.

President Obama has also heard all the reasons why a national EHR can't be done. But a true mark of a great leader is one who is not afraid to take on impossible or unpopular goals and inspire those who can solve the problems to do so.

We have six years to solve our problems. We are seeing our industry roll up its collective sleeves and get to work on them.

One of the first strategies the industry is developing and deploying in this national effort is the Nationwide Healthcare Information Network (NHIN), which is the ultimate Private Cloud with a single purpose use.

The NHIN will connect with regional Health Information Exchanges (HIEs), which will, in turn, connect local medical providers' Health Information Technology (HIT) systems creating one nationwide medical-use-only super data highway.

Some have asked why we just don't use Internet cloud computing, such as Microsoft, Google, or Amazon are currently offering. The answer: the Internet suffers from millions of users who have thousands of uses. This can cause slow downs, delays, and security problems that are not possible to mitigate.

A vivid example is when Google recently made a simple change to its Google Apps database, which allowed data sharing across all domains by all users. The first problem was these domains were supposed to be "forever separated by the virtual software running common applications on shared databases."

The next problem was timing. It took Google Security three days to admit this might be a Google error; before they claimed their change control testing proved the error had to be user, not applications-based.

It then took Google another 10 days to sort through the various affected documents and domains to determine ownership and then restore privacy. During those 13 days, each affected business had no way to know who was accessing, changing, or copying their internal business documents.

When it comes to healthcare, the recent changes in the American Recovery and Reinvestment Act of 2009 (ARRA) to the Health Insurance Portability and Accountability Act (HIPAA) have created a "crisis of trust" in cloud computing for healthcare CIOs. The Act establishes tiers of penalties based upon:

- Whether a covered entity (including physicians) knew of a breach of privacy
- Whether the breach was due to reasonable cause
- Whether the breach was due to willful neglect

The tiers of penalties are as follows:

- $100 / violation not to exceed $25,000 / calendar year
- $1,000 / violation not to exceed $100,000 / calendar year
- $10,000 / violation not to exceed $250,000 / calendar year
- $50,000 / violation not to exceed $1,5000,000 / calendar year

These penalties now include "data at rest," which means any data storage device is now subject to HIPAA standards and needs to be encrypted. For the first time backup tapes, off site virtual storage, USB drives, laptops, CD, DCD, and even equipment being moved from one location to another must have encryption.

There are also a growing number of state and international requirements that exceed HIPAA. Some are even requiring data to stay within certain geographical areas. For example, the European Union places strict limits on what data can be stored by its citizens and for how long. Many compliance regulations require that data not be intermixed with other data, such as on shared servers or databases.

However, many are now turning to "trusted cloud" providers who can demonstrate the needed core services and experience. These include the following:

High-confidence user authentication processes. It takes a provider who works routinely with banking, government, and healthcare customers to fully understand the role that user authentication plays in HIPAA data breach failure and how important it is to provide a safe, user-friendly way to provide for needed access.

Regulatory compliance. A trusted cloud provider has to know the full aspects of regulatory compliance and have procedures to prevent and correct any failures.

Data location. A HIPAA requirement is to know who has access including physical access. In addition, it must know local, state, and national rules for data location.

Data segregation. Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective, however, the service provider needs to prove specialists with Healthcare applications experience designed and tested its encryption schemes

Recovery. There will be outages, accidents, even natural disasters. Therefore, the service provider must have multiple sites for its EHRs to prevent "single failure sites."

Investigative support. The service provider must have auditing, investigating, preventive, and post-incident expertise.

Long-term viability. The old Application Service Provider (ASP) days when clients lost data as a result of a vendor going out of business is still very fresh in CIOs' minds and left a long-lingering fear of "offsite" applications.

Lastly, a somewhat new core requirement:

Data migration and data destruction. The proven expertise to take data from one generation of storage to another is critical because the EHR is a "cradle-to-grave" record.

Data destruction is one of the more important aspects of a trusted cloud provider. When data is erased, it doesn't mean it is gone for good. It still can create HIPAA nightmares. A recent survey by a data security company that bought used disk drives showed that more than 75 percent had "readable" data, including Personal Health Information (PHI), which had been deleted, but not destroyed.

Being a good healthcare CIO means "being passionate" about the stewardship of a patient's data. Today's CIOs understand how important it is to be a control freak about their healthcare data, while at the same time constantly striving for cost controls like those offered in a trusted private cloud.

Trust has allowed Dell Services to become one of the largest providers of IT services in healthcare including cloud services. A number of years ago Andy Grove, CEO of Intel, created a motto that has served healthcare CIOs for years:

"Only the paranoid survive."

With the new changes in healthcare, that motto is even more accurate today.

For more information about any of our service offerings, please contact your Dell representative or visit dell.com/services.