IRON MOUNTAIN®

GRAY CONSULTING

WHITE PAPER

The Anatomy of a Vendor Neutral Archive (VNA) Done Right: **The Case for Silo Busting**

By Michael J. Gray, Principal, Gray Consulting, June, 2011

Sponsored by an unrestricted grant from Iron Mountain

Contents

Summary

The heterogeneous PACS environment is fast becoming the unwieldy beast. This scenario is becoming increasingly expensive to support, and the rapidly rising volume of medical image data is quickly outpacing the limited functionality of the traditional departmental PACS archive. Various other problems are associated with departmental PACS as well. Most notably, the introduction of somewhat proprietary metadata into the DICOM header can limit interoperability with other PACS. The thin-client, DICOM-dependent Clinical Viewer featured by most PACS is no longer suited to the role of the enterprise universal viewer. Furthermore, the strategy of interfacing multiple clinical PACS viewers to the Electronic Medical Record (EMR) system's physician portal is misguided and unlikely to encourage meaningful use.

Since 2006, the concept of an enterprise-class Vendor Neutral Archive (VNA) has gained momentum, as its primary focus is on enterprise image data management and the resolution of problems associated with departmental PACS. The VNA takes over long-term image data archiving from all of the individual PACS, and the associated UniViewer takes over enterprise image distribution and viewing. The VNA assures interoperability among disparate PACS, effectively eliminating costly data migrations every time a PACS is replaced, and gives ownership of the data to the organization, which effectively neutralizes the lock-in strategies of the PACS vendors.

Although there are solid technical arguments for deploying a VNA, the demands for data availability require a mirrored configuration: a primary subsystem to support all of the PACS-to-VNA operations and a secondary subsystem that addresses the disaster recovery and business continuity issues. Properly configured, the VNA becomes much larger than the organization's largest PACS. And, because it is considerably more sophisticated than a departmental PACS, additional IT staff resources with extensive skills will be required. The real question, then, is whether the properly configured VNA is an investment worth making. Can the VNA be more cost-effective than a heterogeneous PACS environment?

Careful cost modeling raises several key considerations. Should the infrastructure be capitalized or operationalized? And should system support be self-managed or outsourced via a Software-as-a-Service (SaaS) contract? Perhaps the most significant consideration is how much of the data should be managed (or has to be managed) on premise versus off premise. What is the potential role of public cloud infrastructure in the deployment of a VNA?

The vast majority of healthcare organizations in the U.S. are failing to mitigate their disaster recovery risk.

There are plenty of good reasons why an organization should deploy a VNA and thereby take ownership of its image data. But the question is, can an organization afford to deploy and operate a properly configured enterprise archive? For many organizations, especially those with limited IT resources, perhaps the only workable configuration is the hybrid VNA. Placing the entire secondary copy of the data and the disaster recovery and business continuity solutions in the cloud can result in a 30 percent lower Total Cost of Ownership (TCO), making the hybrid configuration a financially attractive strategy. This paper reviews the technical arguments in favor of the VNA and presents the results of an extensive cost model developed by Iron Mountain that confirms the financial viability of the hybrid VNA.

Background

It's been nearly three decades since several hundred enthusiastic pioneers gathered in Newport Beach, California, to share their ideas for transforming radiology from a film-based operation to a completely digital operation. Someone suggested Picture Archiving and Communication System (PACS) as a name for this new digital imaging system. Today, nearly 100 percent of the hospitals in the U.S. with 100+ beds have a radiology PACS; 84 percent have it implemented in multiple locations in their enterprise; and 16 percent are single-hospital PACS implementations. Overall, 59 percent of the 100+ bed hospitals have a cardiology PACS (CPACS).[1] Other imaging departments like ophthalmology, dental, and pathology are at least planning for, if not already deploying, their own departmental PACS. In some cases, the imaging departments that followed radiology made arrangements to forward the image data from their departmental PACS to the radiology PACS for long-term archiving. In most cases, each of these departmental PACS ended up with its own dedicated archive. As a consequence, the vast majority of healthcare organizations has this heterogeneous mix of digital information systems, each with its own data management system and archive storage solution.

1 http://www.healthcareitnews.com/news/pacs-adoption-has-reached-mature-stage-study-says

THE PROBLEMS

A number of significant problems exist within this current landscape, dotted as it is with heterogeneous PACS.

Rising Costs Coupled with Explosive Volume Growth

Cost is perhaps the most obvious problem. Rising costs are associated with managing image data in individual departmental PACS, including dedicated data center infrastructure, support staff, disparate storage solutions, and replacement of obsolete infrastructure every few years. Then there's the rising volume of data. Study volume in the U.S. is generally believed to be on the rise again following a drop-off due to the Deficit Reduction Act of 2005, which was implemented in 2007. The volume increase is due both to the aging baby boomer population and the tendency of the imaging procedures to create more images per study. A dramatic rise in data volume is the real problem. According to a 2011 study conducted by the Enterprise Strategy Group, clinical image data volumes will increase by a mind-boggling 42% CAGR from 2010 to 2015. This rising volume of image data will quickly outpace the limited Information Lifecycle Management (ILM) capabilities of the typical departmental PACS, because most of these PACS have outdated backup and disaster recovery processes, and they have no ability to purge or manage the lifecycle of the data.

Achieving Meaningful Use

There is also the problem of how to comply with the Federal Government's Meaningful Use objectives, when each of the departmental PACS' viewing applications require individual interfaces to the EMR system. Having to use multiple viewers, each dedicated to its own imaging specialty, and having to view all of the patients' medical images in separate viewing sessions is the antithesis of simple and efficient. This approach will clearly present a challenge for the physicians to achieve Meaningful Use.

PACS Limitations

In the midst of these obvious issues, the PACS vendors offer little recourse. Their current-generation PACS provide improvements in departmental workflow and diagnostic tools, but they lack technological innovation. Their data management scheme clearly reflects the overall strategy of vendor lock-in, and their recent marketing efforts to reposition their PACS archives as "vendor neutral" are more wordsmithing than fact.

Disaster Recovery Risks

The vast majority of healthcare organizations in the U.S. are failing to mitigate their disaster recovery risk. They are placing too many eggs in the same basket. If they have even a second copy of their data spinning on a separate system, there is weak geographical separation of these systems. Deploying the disaster recovery system in the same building, across the street, or even across town, is simply not good enough. And, if the organization ever had to rebuild a major part of its primary archive from the disaster recovery copy, few have invested in sufficient infrastructure to achieve a reasonable recovery time.

Complexity

A few more vexing problems with today's departmental PACS have been there all along, although largely out of sight. Despite the maturity of the Digital Imaging and Communications in Medicine (DICOM) standard object format for medical images and wide-scale conformance to the standard by the PACS vendors, each PACS introduces its own idiosyncrasies into the DICOM header that sits in front of the image's pixel data. These idiosyncrasies effectively make the image data somewhat proprietary to the PACS that originally acquired those images and somewhat incompatible with another vendor's PACS. These idiosyncrasies can be reconciled when the data is migrated from the old PACS to the new PACS, but short of the wholesale data migration, exchanging data between two PACS on a daily basis is complicated, and full interoperability between disparate PACS is rare. PACS are simply not designed to be open systems, and they tend to hold the data

close to the proverbial vest. Accessing the data from outside of the PACS is challenging. PACS to PACS and PACS to outside physician is overly complex, almost as if the vendor and not the organization owns the data.

In many organizations, the absence of a useful Information Lifecycle Management application, and notably a reliable purge mechanism, has largely gone unnoticed until the data volume under management started to approach 100 terabytes. Since most PACS do not support a data purge application, how much precious disk space is being occupied by image data that has exceeded its legal retention period? Furthermore, the issue of retention and risk associated with keeping data beyond the retention period is often not considered, but it probably should be. In the absence of a purge strategy, other useful ILM policies could at least transfer older data to less expensive and lower performance media. Even today's PACS are simply not designed to efficiently manage the volume of image data the organization has accumulated and continues to generate.

THE SOLUTIONS

All of the above-mentioned problems with departmental PACS have been manifesting for many years. In 2006, the first generation of a deliverable "neutral archive" appeared in the market. The so-called "PACS-Neutral Archive" or "Vendor Neutral Archive" proposes to take the "A" out of PACS. The Vendor Neutral Archive, or VNA, is literally designed to rectify all of the problems with departmental PACS, both those related to data management as well as those related to enterprise image distribution and display.

From the very beginning, the VNA was designed to be the single, central, long-term archive for all of the departmental PACS. The VNA takes over data management from the PACS once the study has been acquired and interpreted. Instead of archiving the data on its own storage solution, the PACS forwards it to the VNA. Mindful that the VNA is supposed to solve these pesky PACS problems, the VNA is typically configured as two identical subsystems, a primary and a secondary. If the secondary subsystem is passive, it is effectively the disaster recovery solution. If both the primary and the secondary subsystems are active, the secondary can share the workload with the primary. And, in this case, both subsystems act as each other's disaster recovery solution. In addition to the level of hardware redundancy in both the primary and secondary subsystems (illustrated on page 5), there is complete software redundancy as well. A mirrored configuration is not only a solid disaster recovery solution, but it is also a business continuity solution, as either subsystem can perform all of the functions of the neutral archive on behalf of the other.

A block diagram of the typical departmental PACS would be a stark contrast to this configuration, as there would rarely be two identical subsystems, two spinning copies of the data, and two instances of the PACS application. If the PACS goes down, the disaster recovery solution is largely useless and there is no business continuity.

The typical VNA supports a sophisticated ILM application that can move image data between various tiers of storage media based on metadata filters — current data is kept close at hand, and older data is moved to less expensive media. These ILM filters can also be used to execute the organization's retention policy, purging image data that is beyond its legal retention period and retaining pediatric, mammography, and any other study types that the organization must keep.

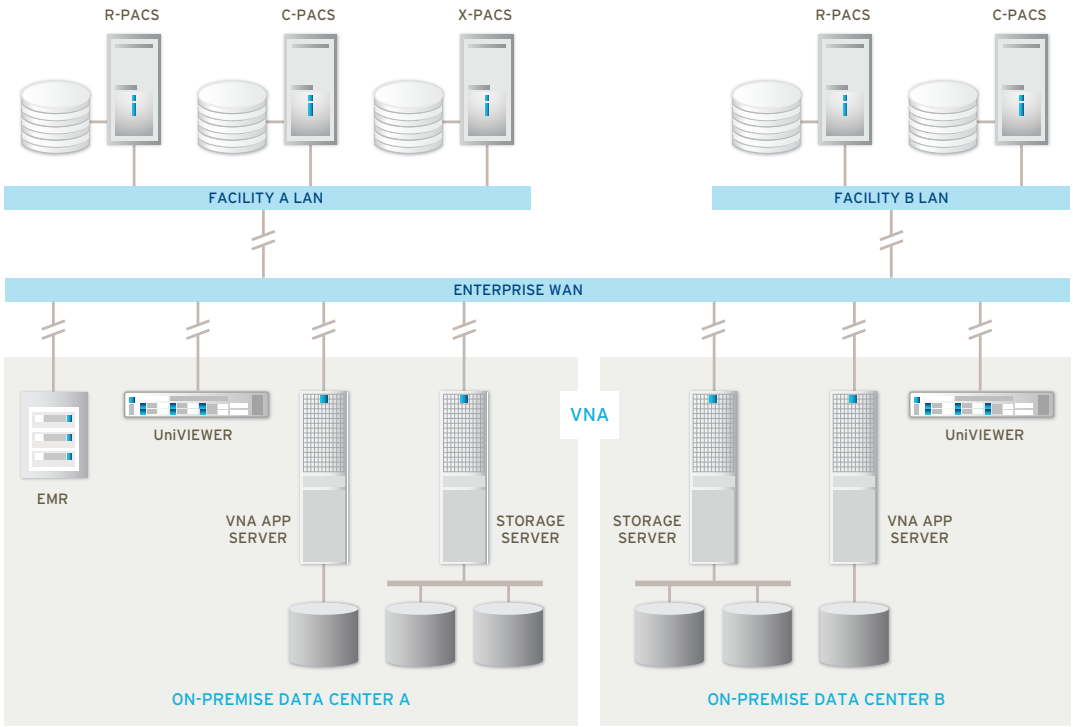
In the block diagram on page 5, you should also note the inclusion of an enterprise viewing application. The term UniViewer has come to represent the class of image display application that can be used by the referring physicians to access and view any image being managed by the VNA through the EMR portal, from anywhere inside or outside of the hospital, using a Microsoft® Windows® or Apple® Macintosh® computer, smartphone or tablet device. It is recognized that a UniViewer most likely will not support the most advanced imaging tools typically

available in the PACS Clinical Viewer, but most clinicians do not need advanced imaging tools. In this regard, the UniViewer has taken over from each departmental PACS the responsibility for distributing across the enterprise and displaying any images being managed by the VNA. The VNA has become the image repository for the EMR.

EIGHT SOLID ARGUMENTS IN FAVOR OF DEPLOYING A NEUTRAL ARCHIVE

1. **Reduced Management Complexity.** The neutral archive allows for consolidation of data management operations. The single-enterprise neutral archive simplifies data management, system monitoring, and system support. The VNA represents a reduction in management complexity — no more managing independent silos, keeping up with multiple storage upgrades, individual hardware refreshes, and various media-to-media and PACS- to-PACS migrations. A single-enterprise archive represents a reduction in software costs and a consolidation of all of the enterprise image data into a single, current-generation storage solution. The VNA has a lower Total Cost of Ownership due to lower costs of storage and storage management, reduced data center costs, and the organization's ability to deal with the large percentage of growth in data volume, with zero or negative growth in staffing.
2. **Interoperability and Data Exchange.** The VNA assures interoperability and data exchange. As more imaging departments deploy their own PACS, and as the organization grows through merger or acquisition, thereby adding disparate PACS to the enterprise, the need for PACS-to-PACS interoperability (data exchange) becomes increasingly necessary. Context management provides the ability to share data and be aware of multiple other disparate systems and their data format requirements such that these disparate systems can be prepared to receive data in a localized manner. A key component of context management is bidirectional dynamic tag morphing. Tag morphing fixes the

VNA ARCHITECTURE



idiosyncrasies in the DICOM header created by the departmental PACS. This function not only enables data exchange between disparate PACS, but it virtually eliminates the need for future data migrations when individual PACS are replaced. Additionally, it is necessary to be able to prepare a PACS to receive data from another PACS. Context Management helps here by providing the appropriate order and patient information, via HL7, between the disparate PACS and RIS systems.

3. **Improved Access to Images.** The UniViewer encourages Meaningful Use of the patient's complete longitudinal medical image record. The UniViewer is a single, multi-specialty viewing application, requiring only a single interface to the EMR portal. Physicians can quickly and easily access and view any image in the VNA from anywhere in the enterprise — on a PC, Mac, smartphone or tablet. This level of performance and accessibility goes well beyond current PACS viewers.
4. **Data Sharing.** The VNA enables data sharing with external organizations and physicians, thus directly affecting patient care and organizational growth. The VNA also utilizes the tag mapping feature, so the data transferred to an outside PACS will be fully compatible with that PACS.

A VNA liberates patient data and shifts back ownership and control to the healthcare provider.

5. **Sophisticated ILM Capabilities.** The VNA gives the organization sophisticated ILM capabilities. The VNA can identify data that can be transferred to different classes of storage. Most importantly, the organization can apply its own retention policies to its image data, and just like the days of the film library, studies beyond the legal retention period can be purged and the storage space reclaimed.
6. **Data Management Tools.** The VNA gives the organization all of the data management tools required to build the complete longitudinal patient medical record, including both structured (DICOM and non-DICOM images) and unstructured data, thus replacing many individual disparate data repositories and viewing applications.
7. **Lower Total Cost of Ownership.** The VNA can be shown to have a lower Total Cost of Ownership than the current heterogeneous PACS environment. We have already reviewed numerous areas of cost savings related to system management and storage, and in addition to those, the costs of future data migrations that are avoided are substantial and deserve their place in any comparison of VNA to heterogeneous PACS.
8. **Take Back Control.** The VNA gives ownership of the data to the organization. Vendor lock-in strategies are effectively neutralized, so the organization can negotiate for any new PACS from a position of true strength.

MAJOR CONSIDERATIONS

Once it is decided that the VNA is the correct strategy for enterprise data management, the next task is determining the best — and most optimal — deployment strategy. The first consideration is the VNA system architecture. The demands for data security require a mirrored configuration: a primary subsystem to support all of the PACS-to-VNA operations and a secondary subsystem that addresses the disaster recovery issue. This secondary subsystem will require a data center geographically remote from the primary, so if the organization does not yet operate a remote secondary data center, a co-location service is a viable option to building a remote data center.

Some consideration should be given to the issue of virtualization. While this requires a higher level of support sophistication, virtualizing the VNA servers not only makes it possible to cut the number of servers required, but the virtualization makes it a lot easier to add server resources as required and to reallocate server resources in the event of server failure.

Careful consideration should be given to the storage solution — both primary and secondary. The incumbent PACS is probably configured with a large percentage of the first copy of the image data on a high-performance storage solution, and it may be tempting to configure the VNA primary subsystem with less expensive, lower-performance media, and even less performance-oriented media for the secondary. While that might make fiscal sense for the duration that the incumbent PACS is managing the bulk of the first copy, when an incumbent PACS is replaced, the opportunity presents itself to configure the new PACS with minimal working storage and have the VNA primary subsystem act as the source for the historical studies. In this case, performance of the VNA storage solution will be critical. The same argument can be made for the secondary, the disaster recovery subsystem. There are many circumstances where retrieval of the image data from the secondary subsystem will also be time sensitive. It is advisable to investigate different types of current-generation storage solutions. First and foremost, it should be an open solution, capable of accepting a variety of storage media. Secondly, so-called smart-storage solutions offer important interface options beyond NFS and CIFS. Higher-performance Web service communications between the VNA and storage will likely start to replace DICOM communications in the next 12 to 18 months.

It is rare for a PACS configuration to feature two instances of the PACS application, so when the PACS is out of service, there is no business continuity. Following the arguments just made for configuring the VNA with robust, nearly identical primary and secondary subsystems, it makes sense to take the extra step of deploying a second instance of the VNA software applications (including the UniViewer) on the secondary subsystem. The disaster recovery solution then becomes the business continuity solution.

Another key consideration is from the IT resource perspective. The VNA is a considerably more sophisticated system than a departmental PACS, requiring the latest OS, database, and network skills, as well as the FTEs for 7/24 system administration, application/operations support, network support, storage administration, HL7, and URL interface support. Whether the organization has this talent and staff count or not, consideration should be given to self-managing the entire VNA or covering support with a Software-as-a-Service contract.

The VNA gives the organization sophisticated ILM capabilities. The VNA can identify data that can be transferred to different classes of storage.

From the financial perspective, consideration should be given to whether it makes sense to capitalize or operationalize the VNA. Wrapping up all of the enterprise image and, possibly, unstructured data management costs into a single operational model can make fiscal sense, while also preserving precious capital.

From the data perspective, some interesting options should be considered. Does the organization physically locate both the primary and the secondary VNA subsystems on premise (the contracted co-hosted data center counts as on premise), or does a hybrid model make more sense, where some significant percentage of the data is located in the cloud? What is the potential role of a secure (HIPAA and HITECH compliant) multi-tenant cloud storage solution offered as a SaaS solution? Consider the fact that the hybrid model can spare the organization the trouble of building or contracting for the second data center. Consider also that moving a significant percentage of data offsite will significantly reduce IT staff resources. If a hybrid model makes sense, an interesting consideration, then, is the ratio of on premise to off premise. There are numerous opinions on this issue, nearly every one of them driven by performance considerations.

Lastly, there are vendor considerations. Archiving is a decades-long proposition. In order to build a favorable cost model, the numbers should be run out through at least two PACS lifetimes to capture the savings associated with future PACS data migrations that will be avoided. Choosing a viable long-term provider is key to a successful enterprise archive strategy. In the end, determining the correct VNA strategy should not be based solely on technical factors, nor be purely a financial decision. The organization should evaluate all of the risk considerations as well, including the viability of the provider.

SYSTEM MANAGEMENT CONSIDERATIONS

As alluded to earlier in this paper, the VNA is a more sophisticated system than the typical PACS. Granted, supporting multiple disparate departmental PACS can be complicated and require an IT team with broad skills because they are all different systems, but at least PACS are comparatively less sophisticated systems. The VNA requires more complex support because it is a more complex system. Specialized expertise and perhaps new full-time equivalents (FTEs) will be required to address the following tasks.

- **Administering the Tag Mapping Library.** The typical VNA includes a user-accessible tag-mapping library based on the vendor's data migration experience. The system administrator can use the library tools to fix any new idiosyncrasies in the DICOM header that may pop up as a result of modality and PACS additions, replacements, or software upgrades. The sooner these updates are made to the mapping library, the sooner the problem is resolved. And, the organization may not be able to wait for the vendor to address these updates.
- **Creating and Managing the Retention Policy.** A system administrator will have to work with the VNA vendor to program the Information Lifecycle Management/Purge application with the organization's electronic data retention policy. Reviewing and confirming the purge logs, and possibly recovering any erroneous purges, could be one FTE, if the volume is large enough.
- **Monitoring the Security Program.** A system administrator will have to diligently review the audit logs and track down any possible security breaches in order to maintain HIPAA and HITECH compliance. Assuming the VNA is feeding image data to a UniViewer which is being used daily by many hundreds of physicians to access and view image studies, this could easily be another FTE.
- **Tracking Multiple System Monitoring Applications.** Most VNA configurations are comprised of multiple software and hardware subsystems, and rarely is there a single, unified system monitoring application. Unless the organization pays the vendor for 7/24 proactive system monitoring, a system administrator will have to keep an eye on the system, and this is easily a quarter FTE.

True Vendor Neutral Archive

As soon as the DICOM standard took hold and prospective PACS customers learned to ask for it, vendors quickly adopted and practiced their one-line response: "Yes, our system supports that DICOM standard." Unfortunately, we've learned that you have to carefully review their DICOM Conformance Statement in order to determine the degree of DICOM conformance. To this day, all of the PACS vendors claim they support DICOM, yet nearly half of the current-generation PACS do not support Presentation States (GSPS) or Key Image Notes (KIN).

Likewise, many vendors have decided to jump on the VNA bandwagon and make claims about their PACS or archive being vendor neutral. Unfortunately, there is no VNA conformance statement, and the Integrating the Heathcare Enterprise (IHE) initiative does not adequately address the requirements of a true VNA.

Following is a list of what constitutes a true VNA. Careful and persistent diligence in ferreting out the truth about a vendor's claims of neutrality is highly encouraged.

- Bidirectional dynamic tag mapping/morphing (because this is the absolute requisite for interoperability)
- Sophisticated ILM and purge capabilities driven by user-accessible metadata filters
- Prefetching (based on user-defined metadata filters used to define "relevancy") and auto-routing to support PACS that cannot query/retrieve from foreign archives
- Ability to ingest and manage both DICOM and non-DICOM image objects
- Accept, manage and exchange all active DICOM SOP Class objects including Presentations States and Key Image Notes
- Provide context management that can manipulate and share all information in an image file, including annotations and notes, which may have been stored in a private header field
- Automatic reconciliation of incoming data with an order or visit
- Reconciliation of multiple Patient/Study IDs without the need for a Master Patient Index (use of fuzzy logic to identify likely matches)
- Enable search of the archive at all four information levels: patient, study, series and image
- Automatically update Admissions/Discharge/Transfer (ADT) information in image files that are already archived
- Support almost any storage environment, so upgrades and replacements can be completed with minimal (if any) impact on clinical operations
- Contractually guaranteed access to the data dictionary and schema, making the customer the owner of the data

- **Storage Consumption Monitoring.** A system administrator will have to use system reporting tools to predict storage consumption and then use this data to create purchase schedules. Unless the organization wants to have 50 percent or more of its storage sitting idle, issuing storage purchases on as frequently as a monthly schedule will require a fractional FTE.
- **The Help Desk.** Similar to the departmental PACS, the VNA and the UniViewer will require a fairly sophisticated and highly responsive help desk, especially if the VNA is managing data acquisition from the smaller imaging departments that do not have a local PACS. The help desk will require both technical and clinical expertise.

Not only will the VNA require new skill sets and experience, it will require additional FTE bodies, as it is unlikely that an organization's current support staff has the required bandwidth. The fact that a VNA is more complicated than a PACS and requires more experienced support staff deserves recognition in the deployment plan.

The VNA should support Remote Access, which, in this case, specifically means the ability for authorized users to gain access and view images from outside of the enterprise facilities.

WHERE THE PACS VENDORS ARE GOING – AND WHY

Most PACS vendors are playing catch-up to the VNA concept, practicing the adage, "If you can't beat them, join them." Unfortunately, a truly neutral archive and the associated UniViewer would limit the functionality of a departmental PACS to data acquisition, department workflow, and study interpretation. This would (should) effectively drop the per study value of a departmental PACS to a fraction of what they are now demanding, so obviously the PACS vendor's strategy has to focus on getting both the PACS and VNA pieces of the deal. Anything less would seriously erode their sales figures and those margins. With few exceptions, most of the major PACS vendors seem to have settled on a strategy of packaging their existing radiology PACS archive as a freestanding enterprise archive subsystem, and creating separate departmental PACS application modules that plug into that enterprise archive. This strategy is not much different than what most of these vendors have been doing the last few years: attempting to graft their cardiology PACS onto their radiology PACS; combining separate directories into one directory; and customizing the viewing applications to the individual departments. After a little wordsmithing and repackaging, you have what is commonly referred to as a SuperPACS™.

Make no mistake. This is still a PACS, with minor (if any) improvements to the same technology that created the header idiosyncrasies and resulting lack of system interoperability that the true VNA resolves. Once an organization starts down the road with a SuperPACS, all of those department modules effectively have to come from that same vendor. One vendor, no matter how large, is highly unlikely to be very good at everything. Organizations that have purchased all of their image and information systems from the same vendor were probably more motivated by financial considerations than technical or clinical merit. While financial considerations are as important today as ever, the rest of this paper will present a better way to make the numbers work without compromising the organization's future with a continuation of vendor lock-in.

ADDITIONAL COMPLEXITIES

A few additional features of the true VNA should be considered requirements, because they will be extremely useful. They, too, will require specialized IT support.

The VNA should be able to accept, manage, and make accessible non-DICOM image data and non-image data. Even a brief description of the acquisition methodology is outside the scope of this paper, but it is important to point out that the acquisition of non-DICOM data is complicated by the associated workflow required to access Patient/Study ID, create an accession number, etc., and the process that builds the proper metadata and associates it with the image or data object. The VNA vendor should offer some solid suggestions and deployed examples for how their system is going to acquire non-DICOM data objects. It is widely believed that Web services will be the preferred interface method, but there is still the issue of metadata creation and association.

It is highly advisable that the organization deploy a UniViewer. The EMR portal viewer will be the primary method of accessing and viewing the entirety of the patient's longitudinal medical imaging record being managed by the VNA. It makes little sense to build and maintain individual interfaces between the EMR and the individual PACS viewers and to force the physicians into learning and using separate PACS viewers. It is recommended that the UniViewer feature a zero-client, server-side rendering functionality. Furthermore, it will be highly useful if this viewer supports both Windows® and Macintosh® platforms as well as smartphones and tablets.

The VNA should support Remote Access, which, in this case, specifically means the ability for authorized users to gain access to and view images from outside of the enterprise facilities. This may require an extension of the enterprise firewall through a virtual private network (VPN) or by means of simple Internet access. The latter will require utilization of data encryption.

Another variation of Remote Access is generally referred to as electronic image sharing. In this case, the VNA supports a mechanism by which outside physicians and organizations can be granted temporary or limited access to the enterprise data. The most useful image sharing applications support access of encrypted data over an Internet connection, and the physician uses the UniViewer to view the images. This is another good reason to select a zero-client, server-side rendering UniViewer, as the nature of the HTML download of image data to the viewing platform is highly HIPAA conformant.

Cloud Infrastructure

The basic idea of cloud infrastructure is that a vendor hosts the storage and server power for the organization off premise, dynamically adjusting your storage space — and what you have to pay for the use of that storage — according to your actual use. The cloud vendor is also providing all of the off-premise system support resources. The local connection to the cloud is through a gateway device (small server with local cache storage) that is located in the enterprise data center. A virtual private network connects this gateway to the off-premise data center and the cloud resources.

There are two major variations of the cloud. The private cloud is dedicated solely to one organization. The server and storage infrastructure could be owned and managed by either the organization or the vendor. The public cloud is owned and managed by the vendor, and the basic infrastructure is shared among multiple organizations. Each organization's data is carefully compartmentalized, so in the case of healthcare organizations, this separation assures HIPAA compliance. The focus here will be on public cloud infrastructure, as this version provides the most appealing cost advantages.

There are numerous applications for off-premise storage, most of them defined by how much of the application's data is kept on premise and how much is moved through the gateway to the off-premise infrastructure. In its most basic form, and in the context of medical imaging, the cloud infrastructure can be an off-premise disaster recovery solution for a PACS or a VNA. Moving any more than the secondary copy of the image data to the cloud is constrained by performance requirements — how fast the local application can access data from the off-premise storage over the VPN connection.

Once an organization has decided that the cloud might play a beneficial role in a VNA, the next important step is to determine the best, most optimized deployment strategy and what the key considerations are for this configuration. What is the mix between on premise and off premise, between capitalized and operationalized, and between self-managed and Software-as-a-Service?

TECHNOLOGY CONSIDERATIONS

The only system architecture issue is the logical demarcation point in the architecture. Assuming the desire to have equal representation of the software applications on both sides of the on-premise/off-premise line, the number of servers in the primary and secondary subsystems would be nearly identical, and the only other architectural issue boils down to how much data is managed on premise versus off premise. This issue is driven by performance requirements.

The performance considerations are largely driven by the required access times for both new and historical data by the PACS users (radiologists) and the UniViewer users (referring physicians). Most PACS would utilize DICOM communications to retrieve historical data from a foreign archive (VNA). Because of the significant overhead of this protocol and the cost and performance of the wide area network options available to the organization, the VNA server and storage managing the historical image data would have to be in close proximity to the PACS servers, that is, on the same local area network. This proximity would be required to satisfy the performance expectations of the PACS users – primarily the radiologists and the specialists who need to access the PACS viewers because of the required toolsets. Furthermore, whether these diagnostic and specialist PACS viewers are fat clients or Web-delivered thin clients, their common characteristic is that they require all of the pixel data to be downloaded to the display platform so it can be operated upon by those advanced tools. Downloading all of the image pixel data from the VNA to the PACS and from the PACS to the display platform requires bandwidth. Hence, the current generation of PACS requires close proximity to all of the new and historical data.

The same argument does not necessarily hold true for the UniViewer users. Even though referring physicians also expect a high level of performance, current-generation, zero-client, server-side rendering display applications will typically access all of the image pixel data from the VNA using the DICOM protocol, but the display operations requested by the user (i.e., window/leveling, zoom, etc.) are performed (rendered) in the rendering servers. Only an HTML (JPEG lossy) version of the image is downloaded to the display platform. Because of this technology, proximity is required only for the VNA and rendering servers; the users can be sitting anywhere.

RISK ISSUES

Data protection (security) is obviously a major consideration. Can the organization trust a vendor to manage its image data in an off-premise cloud infrastructure? This has historically been a tough question for healthcare organizations. There are prejudices and bad experiences. Clearly the organization has to create a list of requirements to be able to determine what data protection requirements should be considered. To start, consider these three major categories of data security that most cloud infrastructure and SaaS providers consistently mention in their sales pitches: administrative tools and controls, physical safeguards (i.e., underground bunkers, biometric locks, etc.), and technical safeguards.

Data availability is a major concern. Will the data being managed in the off-premise facility be available to all user groups, and, if so, how will user authentication be assigned and monitored? How will data access be logged and monitored, and how will potential security breaches be investigated and resolved? Compliance is a very important issue. There are strict and well-defined HIPAA and HITECH requirements for electronic Protected Health Information. Can the SaaS and cloud provider measure up to these compliance requirements? Lastly, there is the all-important reputation and experience of the vendor. Large and reputable vendors are entering the cloud market, but what reputation and experience do they have in managing medical image data?

RECOMMENDATION

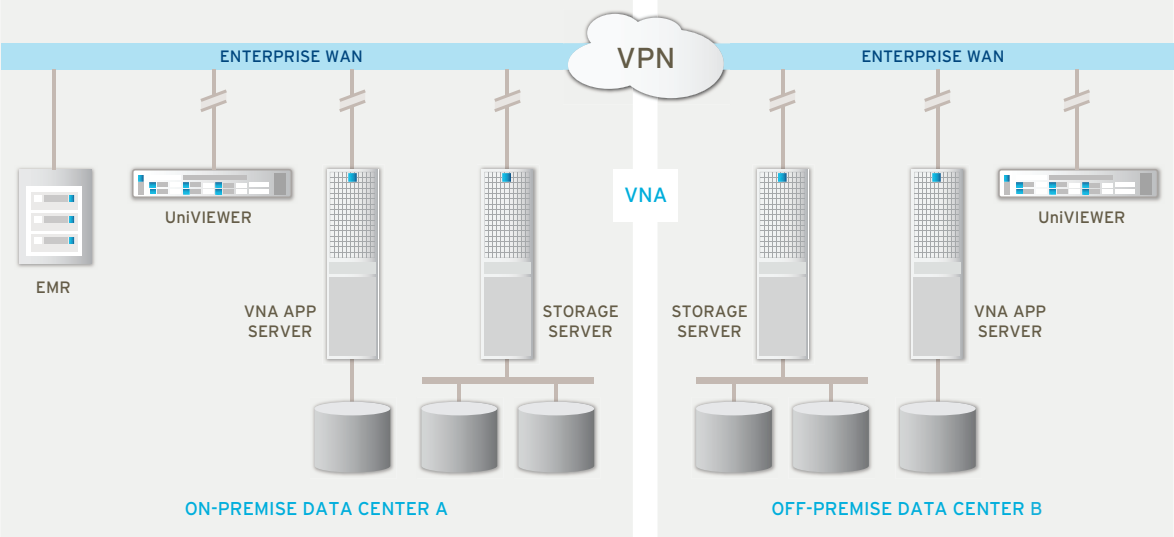
In the context of a Vendor Neutral Archive configuration, the initial recommendation is to keep the primary copy of the image data on premise to guarantee PACS performance, and simply move the entire secondary copy of the data off premise to the cloud. This strategy eliminates the organization's need to build/manage a second data center and the backup server/storage, while satisfying the requirement for a HIPAA-compliant disaster recovery solution. However, in this simplest form, this is only a disaster recovery solution, unless the second instance of the VNA application is also being hosted in the cloud. And, a true business continuity configuration would also have the second instance of the UniViewer hosted in a second location.

Most cloud infrastructure vendors will provide the basic cloud infrastructure, but they are unlikely to be interested in or capable of supporting the organization's chosen VNA application. Cloud vendors that are capable of managing a VNA application are probably not interested in owning and managing multiple VNA applications, as the economic benefits of the public cloud infrastructure would come from sharing a common hardware infrastructure and a common VNA application. Therefore, organizations interested in offloading the ownership and management of the entire disaster recovery and business continuity component of their VNA will have to seek out vendors that in fact are offering a complete hybrid VNA — primary on premise and secondary (the disaster recovery/business continuity component) off premise.

Iron Mountain is one such vendor that is now offering a hybrid VNA. The primary VNA subsystem is located on premise and is connected through a gateway and VPN to the secondary subsystem located off premise in Iron Mountain's highly secure, HIPAA-compliant data center. Both the on-premise and the off-premise applications and infrastructure are owned and managed by Iron Mountain, making this a combination of SaaS and cloud infrastructure. One of several potential Hybrid VNA configurations is presented in the illustration on page 14. The final configuration really is dependent on the customer's environment.

Large and reputable vendors are entering the cloud market, but what reputation and experience do they have in responding to disasters?

SAMPLE HYBRID VNA ARCHITECTURE



As Shown: One of several possible configuration options.

These are a few additional issues to investigate when searching for a viable hybrid VNA provider.

- Virtualized server infrastructure and state-of-the-art "smart" storage solution. Both of these options will assure high availability and scalability while reducing the overall cost per study.
- High security. The vendor as well as the solution should demonstrate HIPAA and HITECH compliance and use of best practices.
- True disaster recovery. The secondary subsystem should be geographically remote, and the data recovery solution should meet required recovery time objectives (RTOs) and recovery point objectives (RPOs) as established by the organization.
- Instead of a VPN connection, users should be able to leverage the Internet for shared access.
- The entire VNA and its infrastructure is provided as a Software-as-a-Service solution. Charges are based on actual utilization, and even the on-premise infrastructure features optimal space utilization.

Following are some of the high-level arguments behind my recommendation to consider the hybrid VNA (as described above) over the on-premise, self-managed, and capitalized VNA.

- The hybrid VNA has a significantly lower Total Cost of Ownership that will be discussed in the next section.
- The hybrid VNA represents a substantial reduction in complexity, as only half of the system has to be accommodated on premise, and all of the management and support is provide by the vendor.
- The hybrid VNA is easier to deploy, as it does not require building or managing a second data center appropriately distanced from the organization's existing data center.
- The hybrid VNA offers a better disaster recovery and business continuity solution, as physical separation is important in a real disaster.
- The hybrid VNA provides the organization with access to the advanced professional services that are required to manage and support a true VNA.

THE BUSINESS CASE FOR CLOUD INFRASTRUCTURE AND VNA SOFTWARE-AS-A-SERVICE

There is a clear potential for cost savings. First of all, there is the transition from a capital model to an operating expense model for hardware and software infrastructure and its management, thus preserving precious capital. Scalability, or, more specifically, the pay-as-you-go storage utilization, creates substantial savings potential over the self-managed, capitalized model, as traditional storage strategies have as much as 50 percent idle capacity being wasted. There is also substantial savings potential in the elimination of various costs associated with the disaster recovery/business continuity subsystem and the requisite second data center.

An argument can be made for a better quality of patient care through the unification of all of the patient's clinical information in a single longitudinal medical record. The implication here is that the VNA application is capable of managing and the UniViewer is capable of displaying both DICOM and non-DICOM image data as well as other key unstructured clinical data that belongs in the medical record. The cloud infrastructure also guarantees the true disaster recovery and business continuity solutions to support that quality of patient care.

The hybrid VNA configuration represents a significant reduction in system complexity. There is no need for a second data center on premise, as the entirety of the secondary subsystem is moved to the cloud infrastructure. The Software-as-a-Service model relieves the organization of some (if not all) of the system support, as the vendor provides system management and support services for at least the off-premise secondary subsystems, and could provide those services for the on-premise primary as well.

You will realize better disaster recovery and real business continuity. The hybrid VNA strengthens the organization's enterprise data management/protection plan. A real disaster recovery and business continuity plan moves the secondary subsystem to a secure, HIPAA- and HITECH-compliant off-premise data center that is geographically separate from the organization's data center.

Resource allocation is improved. Since the hybrid VNA vendor takes full responsibility for system management and support, the organization may assign valuable and scarce IT personnel resources to other projects. The hybrid VNA model also centralizes analytics, including the monitoring of storage utilization, backup progress, network performance, etc. Additional benefits include value-added services such as routine updates to the tag mapping library, resolution of interoperability failures, audit log monitoring and follow-up of security breaches, and execution of imaging-sharing services with outside users and organizations.

The hybrid VNA configuration represents a significant reduction in system complexity.

FINANCIAL CONSIDERATIONS

As was the case with the early PACS deployments, a solid technical argument has to be supported with a solid financial argument. The early PACS adopters often struggled to build a positive financial argument for replacing the film-based operation with computers and display monitors. It's quite possible that many of those initial PACS installations did not meet their financial projections, and yet here we are today with 100 percent saturation in the 100+ bed hospital market because PACS was such a good idea that it became a brick-and-mortar decision. The Vendor Neutral Archive will also probably become a brick-and-mortar decision because it, too, is a very good idea, and its attainment of that status will only be accelerated if we can demonstrate a positive financial argument.

At first glance, moving all of the image data out of each departmental PACS and managing that data in a separate additional archive would seemingly be a cost-plus initiative – until you look at the details in a comprehensive cost model. It has been my experience that a properly designed, on-premise, self-managed Vendor Neutral Archive can be demonstrated to have a lower Total Cost of Ownership than the traditional heterogeneous departmental data management systems (departmental PACS) with their dedicated archives. If the costs associated with the current heterogeneous operations are known, they can be compared with the same line-item costs associated with the VNA and zero-client UniViewer. The TCO for the VNA will typically be lower than that of the PACS, simply because this strategy consolidates the storage, enterprise viewing, and associated infrastructure/support resources. In addition to a lower cost of hardware, the TCO for the VNA will be lower because of the lower cost of managing a significantly lower level of complexity.

It is beyond the scope of this paper to present a complete cost model, but it is important to appreciate some of the major line items in a well-constructed model.

- **Storage.** The storage component is cost neutral. It shouldn't cost more to store the image data in a VNA than in whatever storage solutions are now associated with the PACS, unless of course the PACS is storing the majority of the primary copy of the data on near-line or off-line media. In many cases, storage costs will be less in the VNA because the storage solutions will be based on more cost-efficient, current-generation technology that is probably not even an option supported by the PACS. Furthermore, decentralized departmental storage is more expensive from a management and utilization standpoint.
- **Data Migration.** The cost of the next data migration (to the new PACS or the VNA) is cost neutral.
- **Incremental Costs.** Incremental costs in deploying the VNA include VNA and UniViewer software licenses; servers and related hardware infrastructure; professional services associated with installation, training, etc.; and software and hardware maintenance, including scheduled refresh. A major incremental cost is the secondary subsystem. An appropriate VNA configuration demands mirrored subsystems, and many existing PACS have a totally inadequate disaster recovery solution and a nonexistent business continuity solution.

While the cost of hardware is declining, the cost of managing data continues to climb.

- **Savings.** There are, however, significant cost savings that can equal or exceed the incremental costs.
  1. Storage consolidation reduces hardware and support costs.
  2. Once the data has been migrated from the PACS archives, much of this older hardware can be decommissioned, resulting in reduced data center costs including environmental, power, floor space, and network infrastructure associated with each PACS server and storage solution.
  3. The VNA purge application will continuously reduce the volume of data under management. This reclaimed storage can be used for new study data, so purging effectively reduces the overall amount of storage that has to be associated with the VNA. PACS that are unable to purge data that has exceeded its retention period may be using as much as 20 percent more storage than is necessary.
  4. Costs of future data migrations are avoided. It is important to appreciate that a VNA cost model should run at least seven years, and ten years is typical. The main reason for this is to allow the factoring of one or more departmental PACS replacements. Each of these replacements means an expensive data migration, which of course would be costs avoided in the VNA model. These future costs are inevitable and real, despite the fact they are frequently a point of contention with the CFO. Therefore, they should at least be included, even if they are later discounted.
  5. The costs of developing and maintaining multiple interfaces between the individual PACS viewers and the EMR physician portal are significant, and they are replaced in the VNA model by a single interface between the portal and the UniViewer.
  6. The cost of any future PACS, especially a replacement PACS, will be considerably less when the cost of data management and enterprise distribution and display are removed. Put another way, the organization's negotiating power with the next PACS vendor is substantially enhanced when all of the enterprise data is already in a neutral archive and data management and enterprise display are taken off the table. The value per study of that next PACS should be at least half the price per study of a complete PACS.

Moving a major percentage of data storage to a vendor-managed, off-premise SaaS solution will further reduce the TCO of the VNA.

Once the Total Cost of Ownership for the VNA is understood, it can be shown that moving a major percentage of the data storage and associated system support from an on-premise, self-managed solution to a vendor-managed, off-premise SaaS solution will further reduce the TCO of the VNA and make it an even more attractive alternative to the heterogeneous PACS environment. These additional savings are due to the following:

1. The costs associated with building a second data center, or at least supporting the VNA secondary subsystem in that data center, are avoided.
2. Storage is delivered on an as-needed basis, thus maximizing storage utilization.
3. Capital financing costs are reduced.
4. Capital expenses related to the VNA secondary subsystem are converted to operational expenses.
5. Backup and system management tasks are automated, thus reducing the system support costs.
6. The organization's IT department resources are typically scarce and remain flat, while the volume of work increases. The opportunity cost of allocating resources to the VNA is substantial and may prohibit more strategic initiatives tied to patient care and revenue generation. The value of allocating these IT resources to other strategic initiatives belongs in the TCO model.
7. Software upgrades and hardware refreshes are spread over multiple users of the same multi-tenant infrastructure.

Even a five-year TCO for a hybrid (primary on premise and secondary in the cloud) VNA can be shown to be as much as 30 percent lower than the corresponding TCO for the on-premise, self-managed VNA. The savings increase as the length of the model is increased. Furthermore, there are additional cost savings to appreciate if the organization is in a position to take advantage of a few interesting options that are available from some of the hybrid VNA vendors.

Option 1 is to convert the on-premise primary VNA subsystem to a SaaS solution. This option would convert the capital costs associated with the primary subsystem to operational expenses, and it would reduce support costs by leveraging the efficiency and expertise of the vendor's support staff. The primary storage is also delivered on an as-needed basis, thus maximizing storage utilization.

Option 2 is to move all of the organization's non-image data objects to the cloud infrastructure, thus reducing the costs associated with on-premise management of that data. Non-image data objects that might be moved to the cloud include data from the HIS, RIS, document management systems, email servers, and business applications such as billing, accounts payable, and payroll.

If it sounds simple and straightforward, it usually is not, although reasonably accurate TCO models can be built for:

- A heterogeneous PACS environment,
- An on-premise, self-managed VNA, and
- A hybrid VNA.

The VNA continuously reduces the volume of data under management. PACS that are unable to purge data that exceeds its retention period may be using as much as 20 percent more storage than necessary.

The challenge is that many organizations do not have an accurate grasp of their internal operating expenses, and many of these organizations do not have an adequate disaster recovery/business continuity solution for their existing PACS. Specifically, there is no second data center, or, worse yet, the backup copy of the data is on questionable media and sitting on a shelf. In this very typical case, comparing any version of the VNA to the heterogeneous PACS environment becomes a matter of comparing the expensive "right way" to manage enterprise image data with the less expensive "inadequate way" to manage enterprise data. This could be a tough sell.

In conclusion, when evaluating financial considerations, it is useful to see, at least, the results of a TCO model that compares an on-premise, self-managed VNA with a hybrid VNA with the secondary subsystem in the cloud and all of the systems provided as a SaaS solution. The results are in agreement with multiple vendors' claims of major savings in the hybrid solution.

Iron Mountain has developed a sophisticated and comprehensive TCO model that will compare their hybrid VNA solution with either a heterogeneous PACS environment or a conventional on-premise, self-managed VNA. The model can use hardware, software, professional services, and maintenance costs associated with an actual PACS or VNA, or it can use industry average costs for these line items. If the organization does not know its internal costs of IT support and data center operational costs, the model can draw upon a library of representative local/regional costs for IT resources, data center costs, etc.

TCO FOR REPRESENTATIVE ORGANIZATIONAL PROFILES

Five organizational profiles were created and submitted to Iron Mountain for this exercise. Table 1 indicates the type of organization and the minimum detail required by the model.

Each of the capitalized VNA solutions in this model are configured with a mirrored primary and secondary subsystem. With the exception of the test server, all VNA and UniViewer software applications are represented on both the primary and secondary subsystems. Both the primary and secondary copies of the data are stored on identical single-tier, spinning disk storage solutions. Hardware, software, professional services, and maintenance (including refresh) costs used in the model were supplied by Gray Consulting and are representative of real-world configurations. Each of the

TABLE 1. ORGANIZATIONAL PROFILES

Profile	# Major Facilities (Hospitals)	Annual Procedures	Avg. Study Size (MB)	Annual Growth	Historicals (TB) Uncompressed
A	1 (Community)	200,000	100	4%	82
B	2 (Community)	188,244	82	3%	73
C	1 (University)	163,010	100	3%	81
D	2 (Community)	556,595	78	4%	189
E	18 (Ambulatory)	295,842	68	1%	55

TABLE 2. PROFILE A – 5-YEAR TCO FOR THE CAPITALIZED, ON-PREMISE, SELF-MANAGED, VNA

VNA (On Premise, Self-Managed)	Year 1	Year 2	Year 3	Year 4	Year 5
Storage Hardware Expansion (Years 2-5)	$0	$61,440	$61,440	$61,440	$61,440
Storage Hardware Initial Purchase (Year 1)	$307,200	$0	$0	$0	$0
Storage Hardware and Software Maintenance Contracts (Years 1-3 Included)	$0	$0	$0	$73,858	$82,831
Storage Power and Cooling Costs	$12,587	$14,993	$17,398	$19,804	$22,210
Storage Data Center Facilities	$12,426	$14,801	$17,176	$19,551	$21,926
Storage Administration	$21,152	$25,196	$29,239	$33,282	$37,326
Annual VNA Software License Fees	$34,500	$35,880	$37,315	$38,808	$40,360
Software UniViewer, General Software, and Test System	$131,100	$0	$0	$0	$0
Server Hardware and Infrastructure	$306,538	$0	$0	$0	$0
Data Migration Fees (Reports and Studies)	$258,300	$0	$0	$0	$0
Implementation Costs (Hardware, HL7, DICOM, UniViewer, PM and Training)	$299,406	$0	$0	$0	$0
VNA and UniViewer Hardware Maintenance	$55,177	$55,177	$55,177	$55,177	$55,177
VNA Software Maintenance	$0	$24,996	$24,996	$24,996	$24,996
UniViewer Software Maintenance	$0	$13,600	$13,600	$13,600	$13,600
Totals	**$1,438,386**	**$246,083**	**$256,341**	**$340,516**	**$359,866**

hybrid VNA configurations in this model are functionally equivalent to the corresponding capitalized VNA, and the costs of each were supplied by Iron Mountain. The TCO models for each organization were run for five years.

Table 2 (above) shows the five-year TCO for the on-premise, self-managed, and capitalized VNA configured for Profile A. The storage solution is expanded in Years 2 through 5, but all of the storage volume projected for each year is purchased at the beginning of that year and not on an as-needed basis (i.e., monthly). The three line items highlighted in blue represent the facilities, environmental, and staffing costs associated with the two data centers. Note the large capital investment of $1,438,386 required in Year 1.

Table 3 (next page) shows the corresponding TCO for the hybrid VNA configured for Profile A. In the hybrid VNA, the entire secondary subsystem is moved into the cloud, and the entire solution is provided under a Software-as-a-Service contract. The line items highlighted in gray indicate the facility and environmental costs associated with the on-premise data center. On-boarding refers to

TABLE 3: PROFILE A – 5-YEAR TCO FOR THE HYBRID VNA (SECONDARY IN THE CLOUD AND SaaS)

Hybrid VNA	Initial Year	Year 1	Year 2	Year 3	Year 4	Year 5
Total Storage Cost	$0	$84,130	$140,756	$161,734	$182,318	$202,525
Storage Power and Cooling Costs	$0	$6,294	$7,497	$8,699	$9,902	$11,105
Storage Data Center Facilities	$0	$6,213	$7,401	$8,588	$9,776	$10,963
Total VNA Cost	$0	$67,572	$67,572	$67,572	$67,572	$67,572
Gateway Rental Fee	$0	$5,100	$5,100	$5,100	$5,100	$5,100
On-boarding Costs	$0	$6,684	$6,684	$6,684	$6,684	$6,684
Migration Costs	$0	$2,412	$2,412	$2,412	$2,412	$2,412
UniViewer License and Hardware	$0	$200,331	$0	$0	$0	$0
UniViewer Implementation	$0	$114,752	$0	$0	$0	$0
UniViewer Maintenance License and Hardware	$0	$12,462	$26,062	$26,062	$26,062	$26,062
Totals	**$0**	**$505,950**	**$263,483**	**$286,851**	**$309,826**	**$332,423**

implementation costs for both on-premise and off-premise VNA/storage solutions. Note that there are no upfront costs in Year 1, and the projected yearly costs can be averaged and paid on a monthly basis.

The comparative Total Cost of Ownership for the capital VNA and the Iron Mountain hybrid VNA for all five profiles are presented in Table 4 on page 22. Note that the TCO for the hybrid VNA configuration is lower than the TCO for the corresponding on-premise, self-managed, and capitalized VNA configuration for all five profiles. The percent change ranges from 28% to 36%. Clearly, the hybrid VNA configuration is the more cost-effective way to implement a VNA. But, more importantly, that differential could play a key role in the cost model used to justify the VNA in the first place. If the organization's CFO is unwilling to allow the cost of avoiding future data migrations to be included in the cost justification argument for the VNA, and the resulting TCO for the capitalized VNA then becomes higher than that of the existing heterogeneous PACS, those 30% savings projected for the hybrid VNA may be more than enough to compensate. In short, many organizations may find that the hybrid VNA is the only configuration that makes financial sense.

TABLE 4. COMPARATIVE 5-YEAR TCO FOR CAPITAL VNA AND HYBRID VNA MODELS

Profile	# Major Facilities (Hostpitals)	Capital VNA	Hybrid VNA	Savings	% Change
A	1 (Community)	$2,641,192	$1,698,532	$942,660	36%
B	2 (Community)	$2,542,475	$1,774,422	$768,054	30%
C	1 (University)	$2,663,262	$1,918,597	$744,665	28%
D	2 (Community)	$5,300,505	3,458,356	$1,842,149	35%
E	18 (Ambulatory)	$2,860,199	$1,957,844	$902,356	32%

The TCO for the VNA improves considerably if a hybrid configuration is chosen, and most likely would improve even more if the non-image (unstructured) data objects are also moved to the cloud.

CONCLUSION

The arguments presented in this paper in favor of deploying a Vendor Neutral Archive are compelling, and the strategic move from a heterogeneous PACS environment to a centralized Vendor Neutral Archive with associated UniViewer should not be a matter of if, but of when and how. It makes no sense to continue adding increasing volumes of medical image data in a proprietary format to individual silos. This approach is increasingly expensive, and multiple data migrations are the inevitable consequence. Moreover, as long as the organization does not really own its data, its bargaining position with all future PACS vendors remains weak.

It's hard to argue against deploying a VNA, given the numerous tactical and strategic advantages presented in this paper. The Total Cost of Ownership for an on-premise, self-managed, and capitalized VNA compares favorably to the TCO for the on-premise, self-managed, and capitalized heterogeneous PACS environment – if the organization has a responsible disaster recovery solution and if the organization can accurately assess its operating costs and the CFO understands and accepts the reality of these future data migrations. In this case, the VNA will typically show a lower TCO.

The TCO for the VNA improves considerably if a hybrid configuration is chosen, and most likely would improve even more if the non-image (unstructured) data objects are also moved to the cloud. The majority of U.S. healthcare organizations that do not already have a second data center lack the type of IT resources that are required to manage a VNA as described in this paper. These organizations fully appreciate the benefits of allocating their precious IT resources to other patient care and business initiatives. For these organizations, the hybrid VNA is probably going to prove to be the most common strategy for moving to a VNA.

When the time comes for the organization to build its own TCO model, bear in mind that the fundamental basis for the model should be a true VNA with a mirrored configuration split between two geographically separated data centers and the selection of the right partner/vendor, especially if the hybrid model is chosen. Moving a significant percentage of medical data to the cloud requires enterprise-class security and data protection technology. The details need to be understood and represented in the model, and this paper has presented these key details. Since it might prove difficult getting accurate cost information for the VNA solutions, the best approach is to ask for help. It has been my experience that the leading VNA and cloud vendors are quite willing to lend advice and budgetary numbers.

ABOUT THE AUTHOR

Michael Gray is the principal of Gray Consulting, a consulting practice established in 1991 to develop a number of consulting services designed to assist healthcare systems and radiology practice groups. Gray Consulting has provided consulting services related to PACS and enterprise archiving to over 75 organizations.

Mr. Gray routinely publishes articles on his blog (www.graycons.com) about such subjects as workflow design, business case modeling, system deployment strategies, expansion or replacement of data storage solutions, development of data migration strategies from old to new PACS, as well as the latest market concepts, including PACS-neutral enterprise archiving and the UniViewer based on zero-client, server-side rendering display technology.

Mr. Gray holds a BA in biology and chemistry from Washington University, St. Louis, Missouri. He has been awarded three U.S. patents and has an extensive bibliography in medical image display and electronic information management systems.

Mr. Gray and his family reside in Novato, California.

ABOUT IRON MOUNTAIN. Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company Web site at www.ironmountain.com for more information.