Whitepaper:
VNA Does Not Equal Image Availability - What You Need to Know
## Content

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Executive Summary</td>
</tr>
<tr>
<td>3</td>
<td>Why VNA does not equal image availability</td>
</tr>
<tr>
<td>3</td>
<td>VNA – an incomplete approach</td>
</tr>
<tr>
<td>4</td>
<td>Image protection ensures image availability</td>
</tr>
<tr>
<td>4</td>
<td>Added exposures: XDS and non-image data</td>
</tr>
<tr>
<td>5</td>
<td>Moving VNA in the right direction</td>
</tr>
<tr>
<td>5</td>
<td>Supporting both IT and clinical needs</td>
</tr>
<tr>
<td>5</td>
<td>Storage agnostic archival</td>
</tr>
<tr>
<td>5</td>
<td>Protection through file archival</td>
</tr>
<tr>
<td>6</td>
<td>Summary</td>
</tr>
</tbody>
</table>
Executive Summary

Image protection is a consistent requirement for any PACS system, to guard against image loss. Image loss can occur whenever primary disks fail, when images are corrupted, and when images are erroneously deleted.

Vendors of Vendor Neutral Archive (VNA) technologies have suggested that VNA is a solution to image protection, and that VNA guards against image loss. Commentary from leading analysts including those at Gartner have increased interest in VNA as a means to share DICOM images from one brand of PACS system to another, and have furthered the notion that images held in VNA repositories are made more available. However, many administrators remain unaware that VNA technologies used on their own are insufficient for ensuring image availability. In fact, all images which are held in unprotected VNA repositories remain at risk of loss.

IT professionals including PACS administrators and others responsible for ensuring image availability often use archive technologies as a stop-gap method for preserving images in case of failure. In this case, an archive is used as a kind of backup. These archives are most commonly either dumped to removable media, such as CDROM, or held on spinning disk. Both methods can fail and, therefore, risk image availability. Furthermore, archive technologies are not designed to enable rapid, efficient recovery of managed images.

The two archive methods most commonly in use are:

- Nightly dumps kept on removable media, such as CDROM. These rapidly become cumbersome to manage and are not designed to enable efficient recovery of individual images when needed.
  - In worst case scenarios – which occur frequently – IT professionals and PACS administrators are left with file drawers full of archive media and no sure means to find and recover images.
- Online VNA repositories. On their own these repositories remain vulnerable to failures which threaten image integrity. The most common threats include disk failures and silent disk corruption.
  - In addition, image loss can occur when image files are mistakenly deleted.

IT professionals and PACS administrators need to know that the approach to VNA is incomplete if it does not include capabilities for data protection which ensure image availability. Using a VNA technology on its own to create an image archive does not safeguard those images from loss.

What is needed to ensure image availability is an approach to VNA that is based upon a solid foundation of data protection. In this paper, we will discuss:

- The different layers of archive required to ensure a solid foundation of data protection
- Why the definition of VNA on its own is incomplete and what is missing
- The problem of silent data corruption: Why the most sophisticated RAID protected discs, even when coupled with replication, still cannot guarantee against data loss and corruption
- How to adopt a strategy for your VNA implementation which will support image protection and availability, as well as forming a critical building block to shared access.

Image availability is crucial to patient care. Many healthcare organisations are at risk because their images are not adequately protected. Organisations adopting VNA repositories need to be careful that their approach to VNA is sufficient to ensure image availability. This paper will explain where images are exposed to risk, and how to protect against those risks.
Why VNA does not equal image availability

It may seem counter-intuitive to state that a VNA does not equal image availability. After all, isn’t the market definition of a VNA all about image archival? Unfortunately, the market definition of VNA ignores important requirements needed to provide complete image availability. We’ll discuss how the definition of VNA is incomplete, but first let’s set the stage for that discussion.

To do that, let’s start by looking at the word ‘archive’. Not surprisingly, this word has different meanings to different people. To some, an archive might be a specific piece of storage media, such as a tape or disk archive. To others, this might be a way to protect older files such that they don’t have to be backed up on a nightly basis. Still others might think of a DICOM archive, with the ability to understand how to send, receive and store data defined by the DICOM protocol. Which meaning is correct? The answer depends upon the context in which the word ‘archive’ is used. When you examine the different contexts you realise that there are different levels of archiving, and that they all build upon one another.

The diagram below depicts these different layers and how they work together. We’ll discuss these different layers in more detail later, but let’s begin with a quick definition for purposes of this discussion.

The physical storage layer includes the physical devices that are used to store, or archive, data. The abstraction layer defines how the data is written such that it can be written across many different storage devices, and is often accessed through an API. The file layer views data as being stored in files, and provides archive methods that deal with files of any type, containing many different types of data. The file layer knows about these files, but is unaware of the contents of these files. The content layer often stores its data as files, but is aware of the content within the files such as the DICOM header information in a DICOM image.

Understanding these different layers, what they provide to archival, and how they build upon one another is the key to understanding what is missing in the market definition of VNA, and why VNA does not equal image availability.

VNA – an incomplete approach

Looking at the market definition of VNA and comparing it to the different layers of archival, one can see that it’s an incomplete definition. The traditional definition focuses solely on the content layer, and more specifically on a certain type of content which is DICOM images. The support of DICOM content archival is certainly very important in healthcare, but it must be built upon the other archival layers to leverage their functionality. Focusing solely on the content layer omits archive functionality that is required to ensure image availability.

This is especially true when you consider that data protection is implemented within the three lower layers, and not at the content layer. Vendors who provide a VNA that focuses on the content layer and does not include nor build upon the other layers must do one of two things to provide data protection.

- Partner with other vendors that can supply the data protection of the missing layers, or
- Build data protection into the content layer.

Both methods are common among VNA vendors and both have their drawbacks. Partnering with other vendors increases both cost and complexity, as organisations then must pay for multiple products and manage multiple vendors. In addition, there is the risk that the protection partners selected do not understand, or that they do not support, the specific requirements of clinical users in healthcare.
Building data protection into the content layer also increases cost and complexity, but more importantly often falls short of providing data protection. For example, it is common to replicate VNA implementations across multiple sites. In this approach each site has a copy of the VNA software, and exchanges DICOM images between sites. One site often acts as a disaster recovery site for the other. But replication methods do not include all of the functionality required for data protection. They remain vulnerable to:

- Data corruption when it occurs, either in transit or at rest – and they lack critical capabilities for detecting and correcting data corruption when it occurs
- Day-to-day failures, such as the inadvertent deletion of an image
- The need for rapid image restoration when necessary to support clinical workflow.

As we will see, this functionality is provided by the other archive layers, and it is far easier to build upon those layers with an appropriate approach to VNA rather than build into the content layer. A complete strategy for VNA requires an approach which spans all of the archive layers.

**Image protection ensures image availability**

The previous section discusses data protection as essential functionality provided by the lower three layers of archival. This functionality will be discussed in more detail later, but why is this functionality essential? If images are to be available when they are needed, the images need to be protected against corruption and loss.

But doesn’t technology such as RAID protect the images against corruption and loss? The short answer is that no, RAID is not sufficient to protect images from corruption and loss. The most overlooked vulnerability of relying on RAID is silent data corruption.

State-of-the-art hard drives and disk controllers include hundreds-of-thousands of lines of low-level firmware code. This firmware code has the potential for defects that can cause a more subtle type of disk error which is silent data corruption. Silent data corruption can destroy the integrity of stored images with no indication that an error has occurred. Also, the incidence of silent data corruption is startling. A study of over 1.5 million disk drives over 32 months showed that more than 8.5% of all nearline disks and 1.9% of all enterprise-class disks suffered from silent data corruption. The same study also found that 13% of these nearline disk errors and nearly 38% of enterprise disk errors went undetected by background verification processes.

RAID cannot protect against what it cannot detect. When you consider the growth of image data sets and the increase in disk capacity, corruption of even a single drive can damage a large quantity of imaging data. In these cases, the first indication that an image is corrupted may be when a clinician attempts to use it to support patient care.

Another scenario to consider is that of inadvertent image file deletion. RAID has no concept of “correctness” and cannot stop the inadvertent deletion of data, whether by a user in an application or a user at the operating system level. RAID will delete the data as expected, and if there is no other copy the data will be lost.

In both of these scenarios, a VNA stored on RAID is insufficient to guard against image loss.

**Added exposures: XDS and non-image data**

Another area in which the market definition of VNA proves to be incomplete concerns its support of only one specific type of content: DICOM images. Even when it comes to XDS, VNA vendors only support XDS-I which again relates specifically to DICOM images.

There is much data in healthcare, including images, which are not in the DICOM format. XDS holds the promise of being able to manage much, if not all, of this content, including DICOM. But XDS is in fact, just another content type that, like DICOM, needs to be built upon the other archival layers as a common service. If the content layer is not built upon a common service then functionality like data protection will need to be recreated many times – for each content type and over time, this is just unsustainable.

A complete definition of VNA must include support for all content types, not just DICOM. These must be managed at the the content layer which in turn is built upon all of the layers of archive down to the storage itself. Nothing should be missed if we want a scalable solution that guarantees protection and thereby availability of all the hospital’s data.
Moving VNA in the right direction

Having discussed that the market definition of VNA does not equal image availability, this section discusses the different layers of archiving in more detail, along with the functionality they include. An approach to VNA which is built on all of the archival layers provides a more stable foundation for VNA, allowing VNA to provide for image availability.

Supporting both IT and clinical needs

Before discussing all of the functionality required for image availability, it is worth noting that the definition of VNA must support both IT and clinical needs. These are often seen as independent. Vendors that provide solutions to healthcare IT are often different from vendors that support healthcare clinical users. Part of the reason that most approaches to VNA are incomplete is because vendors focused exclusively on clinical users have capability sets built exclusively at the content layer.

The reverse is also true. However, IT products for data management that are used by healthcare IT are often not defined with healthcare in mind, and as a result ignore the needs of clinical users. Healthcare IT must support clinical users and their workflows, and they need products that help them support those users and workflows.

A common example in imaging is support for relevant priors. Relevant priors are imaging studies that need to be retrieved for comparison with a new study. They provide information on previous conditions or treatment for a patient. If these priors are stored in an archive, it is important that the archive be able to locate and retrieve these priors, as quickly as possible. Failure to do so can have negative consequences on the clinical workflow. A product which is not designed to meet this requirement can leave IT teams without the means to support clinical use of the images.

It is also important to note that a VNA must support multiple departments, such as radiology and cardiology, and that the workflows for these departments are different. Care must be taken to ensure that functionality enabled to support the radiology workflow does not negatively impact the cardiology workflow. It can be tempting to provide functionality in a VNA that corrects problems that exist in PACS relating to the PACS workflow. This functionality is usually specific to each department, and is often not useful, and possibly disruptive, to the other departments. Supporting functionality specific to each department makes the VNA overly complex, difficult to support, and unsustainable over the long term.

It is better for the VNA to focus on the problems relating to archiving across several departments. This keeps the PACS in control of the departmental workflow, and allows each department to select the PACS that best supports their workflow while maintaining a common archiving strategy across all departments.

Finally, clinical and IT needs when understood do not need to be at odds with one another. For example, image availability is important to clinical users, and image protection is how IT maintains image availability to their clinical users.

Often, clinical and IT needs are merely different sides of the same coin. What is needed: better tools which are designed to bridge the gap between what clinicians want and what IT needs to support clinical requirements.

Storage agnostic archival

There are many storage devices available from a wide variety of storage vendors at the physical storage layer, and the functionality provided by these devices can differ greatly. This paper will not discuss the many different devices, their functionalities, or the pros and cons of each. What we will discuss is the need to be ‘storage agnostic’, which is the ability to support any storage device for archiving.

Archiving is used for unstructured data that rarely changes and needs to be kept for long periods of time, often because of regulatory requirements. It is certain that data archived for 10, 20 or 30 years or more will not be stored on the same storage device for its entire life within the archive. In addition, if archived data needs to be retrieved 10 years, or more, later it most certainly will be restored using a different generation of storage hardware.

Also, to protect data from corruption, it is best to archive data to more than one storage media type. It is highly unlikely that the data will be corrupted on both media types at the same time, so if the data becomes corrupted on one media type it can be restored from the other.

For these reasons, data should be archived in a format that allows it to easily be moved from one storage media to another. This is the primary purpose of the abstraction layer. It ensures that data can be archived, and retrieved, from multiple storage devices, making it storage agnostic.

Protection through file archiving

Data protection is provided by the file layer working with the abstraction layer. Unstructured data is most often stored in files. DICOM images, scanned documents, reports, video and results from many different studies are stored as files. The basic file format provides the lowest common denominator for providing archive functionality that is application independent, and which can be protected from loss.

The file format as lowest common denominator, combined with functionality from the abstraction layer provides the basis for data protection. Digital signatures from the abstraction layer applied to files provide the ability to ensure that the files are archived correctly and that files retrieved are not corrupted. When files are archived to...
multiple storage media, the digital signatures are used to detect and correct files that have become corrupted on one storage media. Digital signatures can also be used to detect duplicate files and reduce storage that is allocated to duplicate files. In this way, files including image files are protected from loss through corruption.

Additionally, file archiving can store multiple point-in-time versions of a file created when a file has been modified. This can provide support for regulatory requirements that require the ability to keep prior versions of a file. It can also be used to protect against the day-to-day failures such as when a file is incorrectly modified. A prior version of the file can be restored to correct the inadvertent modification.

But do storage costs go up? The short answer is no. Because data protection requires multiple copies of files, including multiple versions, policy rules can be used to manage the costs of storing multiple copies. Policy rules can be designed to keep older, less used, copies of files on less expensive storage such as near-line disk or tape. Policy rules can be based upon the file name, extension, creation date, modification date, or any other file attribute. Policy rules include retention dates to indicate how long to keep files, and can vary for different media types. An example would be to keep files in onsite disk storage for two years, offsite disk storage for four years and on tape indefinitely.

As another benefit, encryption is used to protect archived copies of data from unauthorised access. Where device encryption is available it is used, but software encryption is also available for protection on devices that do not provide device encryption.

File archival functionality provides a powerful method to protect unstructured data stored in files, and protect those files from loss. A VNA that is built upon a strong foundation of file archive is secured against image loss or corruption.

Summary

The premise of this paper has been that a VNA, as most commonly defined in the market today, does not equal image availability. This is true because most vendors offering VNA capabilities are limited to the content layer, and do not include a solid foundation for data protection. A solid foundation for data protection requires support for multiple layers within the archive. In most healthcare organisations, therefore, DICOM images and other critical healthcare data remain vulnerable to loss and corruption even when residing in VNA repositories.

What’s required is an approach to VNA which bridges the gap between the DICOM content layer and the lower three layers of archive. A sufficient VNA approach must be aware of clinical modalities and requirements, while also maintaining storage-agnostic flexibility with policy-based archiving to ensure cost-effective use of tiered storage systems. Only this unique combination which bridges the gap between what clinicians want and what IT needs provides a sufficient approach to VNA which avoids image corruption and data loss.

BridgeHead Software provides a unique approach to Healthcare Data Management with a platform that is built upon the four layers of archive. It is storage agnostic to allow the use of any storage media available at the physical storage layer. It provides a repository at the abstraction layer with functionality such as digital signatures and encryption that work for all data types and all storage types. It retains DICOM awareness to ensure clinical use of images is supported fully.

It provides the file archival capability to provide protection at the file level, including file versioning, and policy rules based upon common file attributes.

Finally, it supports the standards in healthcare to provide content layer archiving for both DICOM images and standard file types that are commonly found in healthcare.

For more information on the BridgeHead Healthcare Data Management platform and how BridgeHead can help to bridge the gap in your approach to VNA, please visit us at www.bridgeheadsoftware.com.
With 20 years’ experience in data and storage management, and 10 years in healthcare, BridgeHead Software is trusted by over 1,000 hospitals worldwide.

Today, BridgeHead Software helps healthcare facilities overcome challenges stemming from rising data volumes and increasing storage costs while delivering peace of mind around how to STORE, PROTECT and SHARE clinical and administrative information.

BridgeHead’s Healthcare Data Management (HDM) solutions are designed to work with any hospital’s chosen applications and storage hardware, regardless of vendor, providing greater choice, flexibility and control over the way data is managed, now and in the future.

Learn more about BridgeHead Software at www.bridgeheadsoftware.com

Follow BridgeHead Software on Twitter at www.twitter.com/bridgeheadhdm