Medical Imaging

Storing and serving medical images can present numerous challenges. First, files need to be readily available for quick access when doctors and other medical professionals need them. However, these files tend to be extremely large and need to be securely and indefinitely stored both to protect patient privacy and to meet federal guidelines such as the Health Information Technology for Economic and Clinical Health Act (HITECH) and Health Insurance Portability and Accountability Act (HIPAA). It's not just what you are supposed to do – it's the law.

The Panzura Freedom Family delivers:

- Data center performance with the economics, scalability, and durability of the cloud
- Your choice of private cloud and public providers including AWS, Google, Azure, IBM and more
- HIPAA compliant with FIPS 140-2 validated military grade encryption
- In-line deduplication and compression
- Secure Erase

Medical images can be generated by multiple, disparate sources and have typically been stored using picture archiving and communication systems (PACS). PACS are systems that have been designed to connect to specialized medical imaging equipment and to store, transmit, and share those images within a hospital or other healthcare facility. However, PACS can lead to islands of storage, often have interoperability issues even within the same hospital, and can be expensive to upgrade.

Rather than continue to invest in PACS, many healthcare organizations have moved to vendor neutral archives (VNAs) such as those from Teremedica, Merge Healthcare, and DeJarnette. One of the biggest criticisms of PACS is that the images they store are frequently not accessible by other systems. This can result in considerable difficulty sharing images, even across departments within the same hospital, which can impact patient care. VNAs solve this by storing images in a standard format that can be accessed by other devices, regardless of manufacturer.

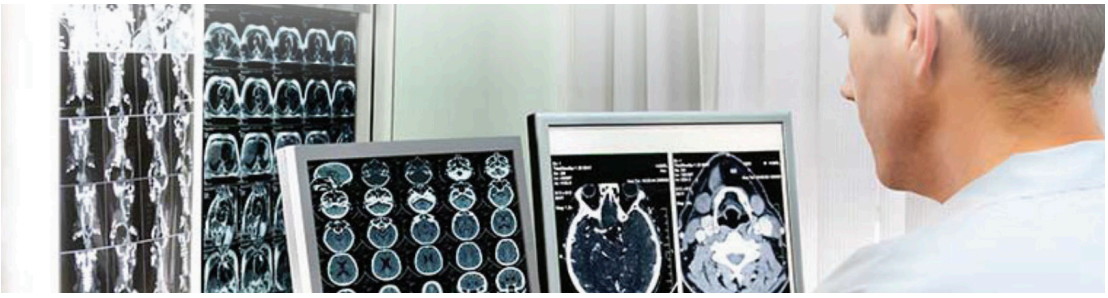
Still, while VNAs may help solve the challenge of bridging data across multiple formats, there are still other challenges that must be addressed. These include security, as data must be protected both against accidental loss and from outside attacks, and scalability as the storage must be able to seamlessly expand to meet the continuously growing need for more capacity.

Medical imaging files can be huge and quickly overwhelm many types of file storage. On-premise filers and NAS devices can act as a high performance image repository, but they are also expensive, require significant management and are limited in their ability to scale. Cloud storage can offer the needed scalability to handle the influx of medical images, but at the cost of performance. Latency between the cloud storage and the healthcare provider, particularly with large image files, can cause unacceptable delays in opening in files and seriously impact patient care.

695 Campbell Technology Pkwy #225, Campbell, CA 95008, USA

Panzura for Medical Imaging: Performance, Scalability, and Security

Rather than forcing users to choose between the performance of local storage and the scalability of the cloud, Panzura offers a best of both worlds option. The Panzura Freedom Family stores image files on scalable, affordable cloud storage, and dynamically caches those files that will be needed quickly on high performance flash memory, and is fully HIPAA compliant.



Since the images are cached locally, they are immediately available to the users who need it to deliver immediate patient care. However, since all data is stored in a scalable cloud based object store, capacity is never an issue. Your cloud capacity can scale on demand to meet your needs. Further, since you can consume storage on demand, there is no need to buy storage in advance of consuming it. Where on premise storage typically requires an investment in capital equipment with a lifespan of 3-5 years, requiring IT to predict how much capacity will be required years in advance, the Panzura solution allows users to only purchase what they need, when they need it.

To further help control storage costs, Panzura Freedom performs deduplication and compression on all files. This reduces the total storage footprint, as well as the amount of data that needs to be transmitted to the cloud. Many installations have seen an overall storage footprint reduction of 90%.

Data security is assured through FIPS 140-2 encryption. Data is protected both at rest and in-flight for maximum protection. Encryption keys are never stored in the cloud, so users always remain in control of their data. In fact the security is so strong, that it has been adopted by the National Institute of Standards and Technology (NIST), the federal organization that certifies FIPS compliance. Strong encryption and data protection capabilities are why Panzura Freedom is certified as HIPAA compliant.

Further, the HITECH standard not only includes requirements for data in motion, at rest and in use, it also sets forth details on how the data must be disposed of when it will no longer be stored. Panzura includes a secure erase option that is most secure data disposal method available today, short of the physical destruction of the device the data was stored on.

For more in-depth information medical imaging archive or medical imaging storage, please check out the Panzura Freedom Solution Brief. Also, see how the American College of Radiology replaced EMC VNX, replication, and Data Domain by using Panzura and cloud storage.