Vault Computer Secure Data IP Plan

For Healthcare and Insurance - HIPAA Compliancy

Almost all medical data and information used by the healthcare and insurance industry is digitalized in some form. How do you protect healthcare and insurance data from today's realistic and ever increasing intrusion and threats; and be HIPAA compliant?

To answer this question let's review the three major causes for data loss:

1. Hardware Failure
2. User Mistakes
3. Theft

Vault Computer's primary goal is to keep your data secure. Whether you handle healthcare, government, industrial, business or personal data our computer platforms gives your data unbreakable protection.

What Makes Vault Computers different?

Using the above causes of data loss let's examine what Vault Computer designs achieve in each case.

1. Hardware Failure – This is the most common cause of data loss and it is the easiest one to combat by utilizing quality. Vault Computer uses the highest quality components available today – that is why they cost a little more. The biggest enemy of computers is heat. The heat computers produce can be acute or over time, destroying motherboard components and attached internal devices. Either by direct heat damage or long-term expansion and contraction your components will erode and fail from exposure to heat. We use high durability motherboards that are twice as thick and have twice the copper for rapid heat dissipation and low expansion. The typical motherboard in a $1000.00 computer costs about $20. For a Vault Computer motherboard we spend a great deal more to bring you advanced designs with a long service life and dependability.

Average computer temperatures run in the 48° - 55°C range. Our top Power/Server model runs at 25° - 28°C implementing our excellent air cooling design. This means long-term service life and dependability. All of the components we use in a Vault Computer are the best quality we can find. The hard drives are Enterprise Level and carry a 5-year manufacturer's warranty. Vault Computers are designed to operate cool and quiet.

2. User Mistakes (Oops) – This is the most difficult issue to combat because most of the problem depends on a users' behavior and training. What we at Vault Computer can do is make it easier to recover data through backups from independent drives and cloned Operating System (OS) drives.

Vault Computer offers the options of having a cloned OS drive and internal independent backup drives. To implement these features all of our computers are configured with **hotswap** capable systems. This means you can turn on and off a hard drive that is separate from your OS operating drive while the computer is running. This keeps that drive secure and unaffected by any invading software or hackers. It also eliminates unnecessary wear and energy consumption. You can recover your problematic operating system from a pristine cloned copy you have reserved in about 6-12 minutes. No more hours of virus, malware and spyware scanning or reinstalling your operating system and programs. This method helps prevent "down time", thus saving time and money.

If you ever suspect your operating system is compromised you can delete it and recover with your backup clone copy and be back in operation within minutes.

You may also hotswap your secure backup drives for updating or recovery of data. Keeping these drives offline not only saves energy and wear but keeps them separated from potential corrupting software codes and are invisible to hacking.

3. Theft – This is the fastest growing cause of data loss today and the easiest to combat with our new technology! Vault Computer offers the full **hardware encryption** option. The entire hard drive and operating system employ government level 256-bit AES hardware encryption. Additionally, we use CBC (Cypher Block Chaining) which offers 4 quadrillion times more security than the approved government level ECB (Electronic Code Book) encryption. Hardware Encryption

is a brand new patented technology protecting your data in ways never before achieved. All other forms of encryption to date are software encryption. For a more thorough comparison of Hardware Encryption vs. Software Encryption see the appendices.

The first and most obvious difference with an Encrypted Vault Computer is that there is no "foot in the door" with new hardware encryption. The computer will not boot up without the proper key inserted. This means no hack tools are possible - there is no back door. You can now control who uses the computer and who sees the data on it. A higher level of responsibility is achieved from users.

Moreover, if the computer is stolen or the encrypted hard drive is removed it will not reveal any data. No forensic techniques can be applied and your data is secure from unwanted investigation. **The data is invisible, irretrievable, unbreakable and secure from unauthorized access – period.**

Vault Computer Designs

Vault Computers are customized for your needs from our base models. The Government Workstation Model handles all light to medium loads with ease. It features a 4-core processor that tops out at over 4 GHz/core with 16 GB of DRAM. It has HD video and sound.

The Power/Server model can handle the heaviest loads and may be equipped with an 8-core processor and 32 GB of DRAM. It can be customized with up to 48 terabytes of internal storage and with up to 48 additional terabytes attached. It is designed to transfer huge volumes of data simultaneously with other tasks running. It is a workhorse that will save both time and money for your organization.

Both models feature USB 3.0 (10 x faster than 2.0), eSATA, 6 Gb/sec SATA interfaces, special fans and a powerful modular silent power supply.

Healthcare Data Usage and Storage – HIPAA Compliancy

All healthcare data requires security and uncompromised handling to ensure HIPAA Compliancy. End user computer stations and the servers storing essential data require restricting unauthorized individuals from accessing healthcare data. You will need only minor training to manage the requirements and protocols. All our computers are HIPAA compliant.

We recommend a two-phase approach. **First, store you data in encrypted form and under your control.** This can be achieved by using Vault Computer's Power/Server model that will process your data fast and into encrypted containers (up to 8TB each) using the onboard hardware encryption engine and SATA dock. This model can house up to 48 TB. Encrypted NAS storage may be added at 24 TB each.

This hardware encryption engine can use its own key code for data storage providing extra control and security. Once a cataloged container is full it can be stored under your control, as a library or available online in your server, for future retrieval and use. This eliminates waiting and the risks of transfer from other locations.

The next phase of **optional** storage involves a secondary encrypted backup to a dedicated storage facility. This may be required for additional data security. We do not recommend using cloud-based storage model services. These cloud-based storage systems suffer numerous failures. For further education on cloud storage weaknesses and statistics please see the appendices. Using simple logic one may derive that risk of data loss increases with the number of cloud administrators transferring your data and their company's use of the multitude of ever changing storage leasing centers worldwide!

Vault Computer recommends using offsite secure data storage. We recommend Offsite Vaults at www.angstromlord.com. They employ secure encrypted backups in a dedicated location. Our Vault Computer service team can help you move your data to them.

The end user computer stations are an often overlooked weak link in a secure data system. Busy personnel leave computers on for various reasons and those computers are windows to your entire healthcare or insurance network of private data. In many cases end user workstations are accessible to unauthorized entry by visitors or other staff such as janitors and maintenance personnel. Our computers start and shutdown quickly so there is no need to leave them on due to being slow. Being encrypted denies operational access by unauthorized users and thieves.

If a company computer or hard drive with HIPAA protected information is stolen then your data will be invisible. You will be required to prove under HIPAA regulations that the data is not compromised to thieves or unwanted investigation to prevent substantial fines or sanctions. With hardware encryption the data is always encrypted. Encryption is always on and it cannot be turned off.

We have two models of end user stations. For computers stations with high workloads or more complex use such as technical and multitasking operations we build a Power Model version based on our server architecture. It is fast and will handle the highest workloads. Speed saves time and money on your budget.

For moderate workloads we recommend using Vault Computer's Government Workstation model. This computer is also fast and should also be encrypted to prevent unauthorized access. Both models can be configured with hot swappable storage and cloned OS drives. We will customize our computers to fit your needs.

No matter what data you want to protect from unwanted access, whether its for healthcare, government, industrial, business or personal use, Vault Computers will give you 100% secure data protection

Vault Computer

~

www.TheVaultPC.com

Jim Austin **Telephone: (904) 254-0849**

Vault Computer LLC is a certified

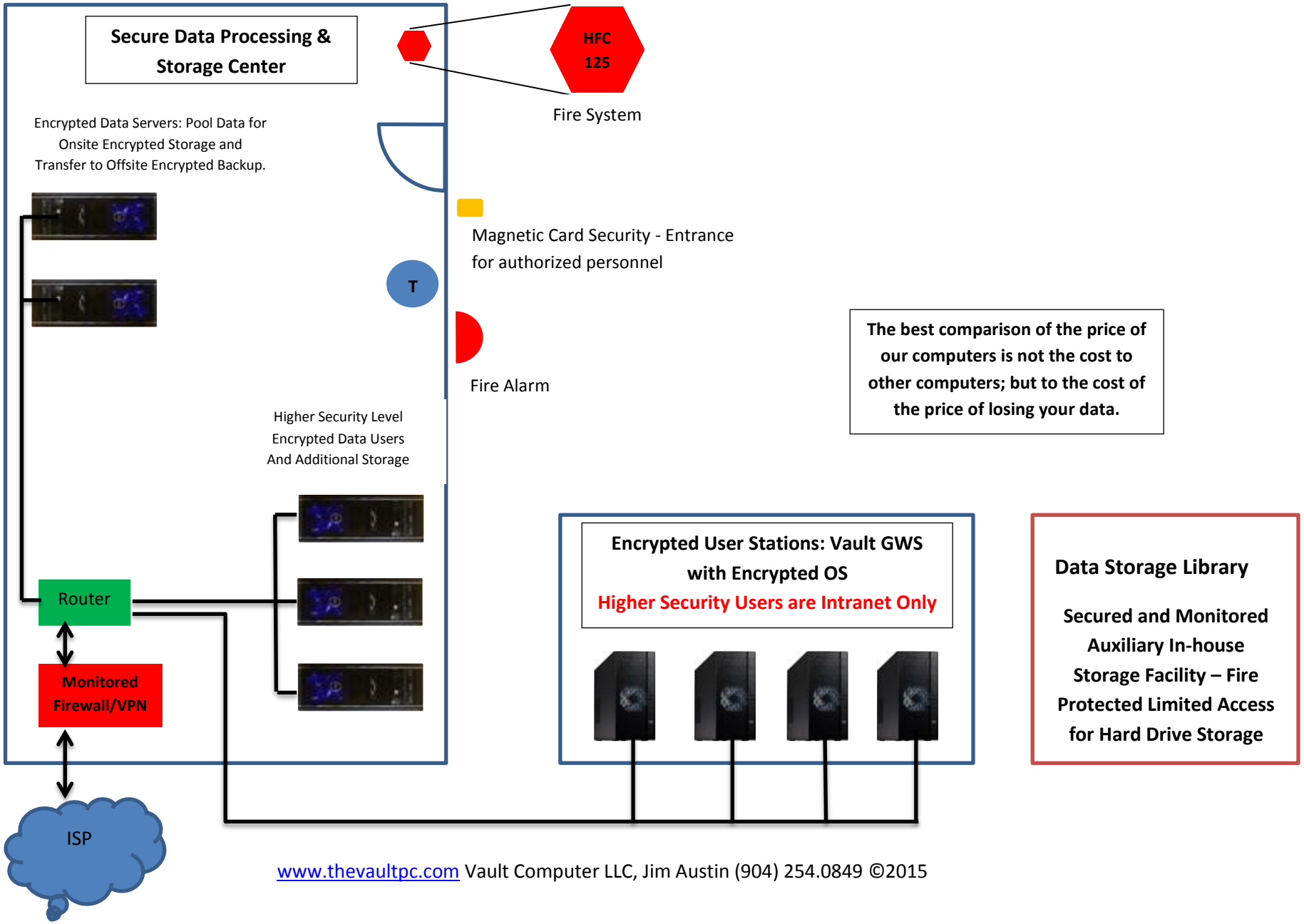
Service Disabled Veteran Owned Business

Our Computers are 100% American Made

Vault Computer is a Certified HIPAA Business Associate

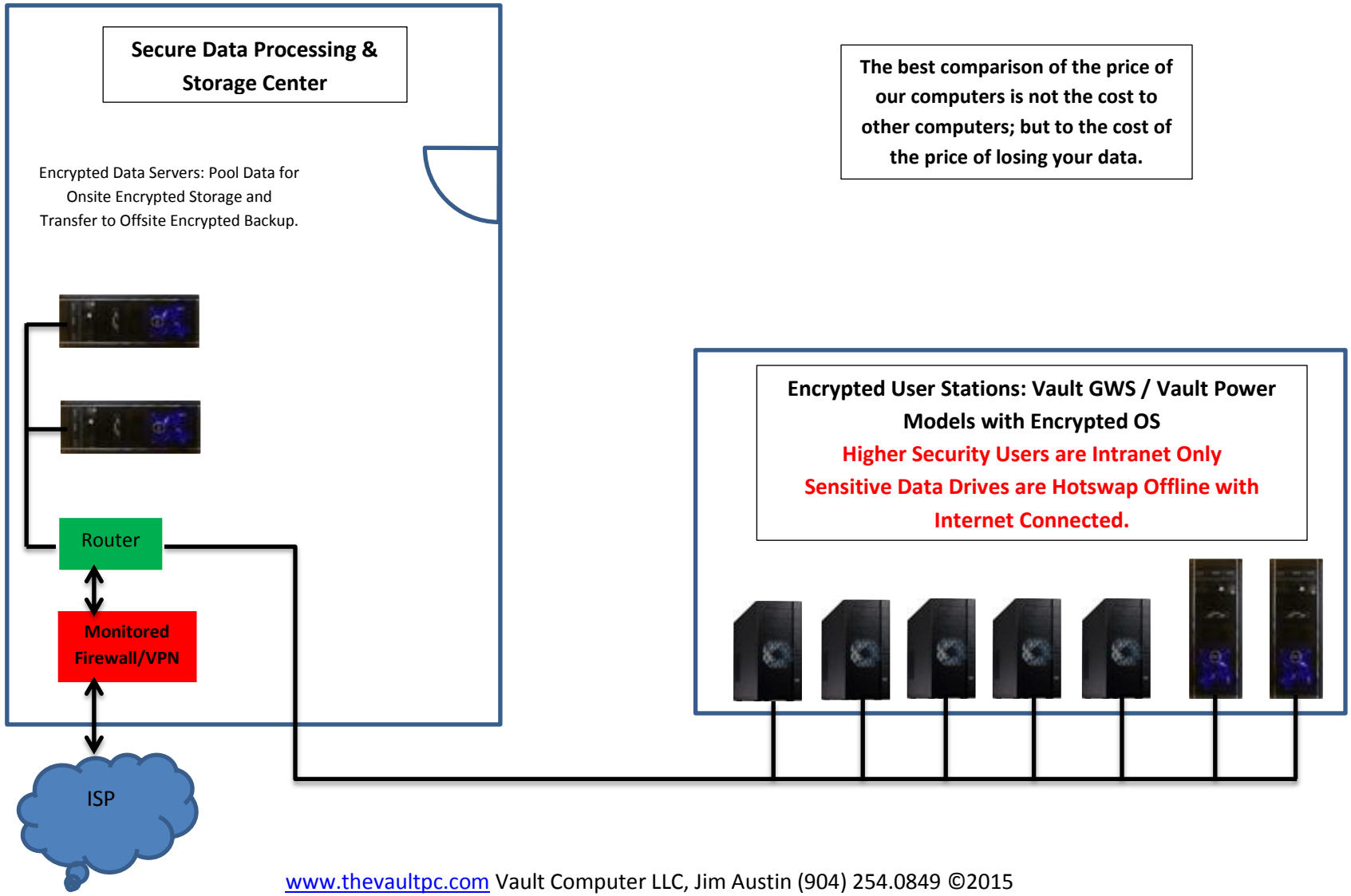
Now let's look at examples of Secure IP Plans for Healthcare and Insurance Data Storage.

Vault Computer Secure IP Plan for Healthcare and Insurance Data Storage



Vault Computer Secure IP Plan for Healthcare and Insurance Data Storage

Simplified Efficiency Model



Appendices

Vault Computer

Advantages of Hardware Encryption over Software Encryption

- No passwords to learn, forget or recover.
- No training needed as with software based encryption. Insert the key and you are operational.
- No software updates – no additional costs or time consumed updating computers.
- Hardware Encryption operates across all OS platforms and there are no program incompatibilities as with software encryption.
- Does not consume CPU resources as does software based encryption. Hardware Encryption operates independently on its own power.
- Viruses, Malware and Spyware will not affect the encryption engine because the encryption is hardware generated and not by corruptible software.
- There are no generated clues (folders, shortcuts, registry keys, etc.) of encryption on the data drive as in software encryption.
- There is no “foot-in-the door” to apply brute force attack, hack tools or forensics. The computer will not boot nor will the drive indicate data.
- NO data is ever visible on the encrypted drive. It will only appear on a normal SATA port as an uninitialized “new” hard drive. This gives “plausible deniability” that any data has been on the drive.
- Hardware Encryption can employ CBC mode encryption. Cipher Block Chaining, is a confidentiality mode whose encryption process features the combining ("chaining") of the plaintext blocks with the previous cipher text blocks. In addition to using a given DEK (Data Encryption Key), the security level of a CBC implementation is quadruple trillions times more than that of ECB (Electronic Code Book) mode found in software encryption.
- Lowest Encryption TCO – Total Cost of Ownership is lower with hardware encryption given that less time, money and energy is needed to operate hardware encryption.

Vault Computer – www.thevaultpc.com

Jim Austin Telephone: (904) 254-0849

According to Symantec's 2013 Report "Avoiding the Hidden Costs of the Cloud":

- 47% of enterprises lost data in the cloud and had to restore their information from backups
- 37% of SMBs have lost data in the cloud and had to restore their information from backups
- 66% of those organizations saw recovery operations fail

According to The Aberdeen Group's Report "SaaS Data Loss: The Problem You Didn't Know You Had"

- 32% of companies surveyed lost data from the cloud.

Of these instances,

- 47% were due to end-users deleting information
- 17% were users overwriting data
- 13% were because hackers deleted info

According to the Cloud Security Alliance's Top 9 Cloud Security Threats in 2013

- Data Loss [from theft] is the #2 reason for data loss (up from #5 in 2010)

According to the Boston Computing Network's Data Loss Statistics

- 60% of companies that lose their data will shut down within 6 months of the disaster

According to CloudBackup's Facts about Data Loss

- 20% of small to medium businesses will suffer a major disaster causing loss of critical data every 5 years. (Source: Richmond House Group)
- About 70% of business people have experienced (or will experience) data loss due to accidental deletion, disk or system failure, viruses, fire or some other disaster (Source: Carbonite, an online backup service)

You may notice that some of these stats actually contradict others. It may depend slightly on the number of companies surveyed, but in general, **companies are not usually eager to admit they have suffered from these kinds of data losses. Telling the world that you accidentally deleted really important information just does not happen unless one's hand is forced. It hits the bottom line through profits and undermines confidence and trust.** But regardless of whether it is 32% or 47%, up to almost *half* of companies have lost important business information in one way or the other — and oftentimes it was accidentally deleted.