

## HIPAA Compliance

Ensure your backup system is HIPAA compliant with **SEMPER VIVO**. Our data storage services qualify as HIPAA compliant.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was enacted by the Health and Human Services (HHS) department to establish the standards for the privacy and protection of personal health information. Personal health information is defined as any individually identifiable health information in any form or media including subsets of health information such as demographics. The HIPAA regulates almost every area of health-related organizations from hospitals to single doctor's offices. The healthcare entities affected by HIPAA include all healthcare providers, employers, public health organizations, hospitals, insurance agencies, clearing houses, billing agencies, service organizations and any one dealing with personal medical information. Non-compliance with HIPAA carries stiff civil and criminal penalties.

HIPAA also regulates the secure storage and transmission of confidential patient data over computer networks. HIPAA privacy requires that only authorized individuals have access to personal health information. It defends the individual right to keep information about themselves from being disclosed. Healthcare organizations are required to take suitable measures to implement electronic data protection both during storage and while in transit. Additionally, HIPAA requires that the integrity, confidentiality and availability of the information be maintained through the establishment and maintenance of appropriate administrative, technical, and physical safeguards.

According to HIPAA regulations, the backup system must be able to survive "an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information".

With **Semper Vivo**, the data is held at our servers. By doing this, the data is located at an off site facility. Should your office be subject to an emergency or other geological threat, patient data is safely stored and accessible in a more geologically sound area. This ensures your backup system meet HIPAA requirements. Of course, you must ensure that your data is being stored on **Semper Vivo's** Infrastructure to ensure true compliance.

Your data is also backed up to tape and stored at a secondary facility. Although, tapes and CD/DVDs back ups don't qualify because they can be damaged or destroyed, they provide a secondary level of security that your data is accessible and safe.

You transfer your encrypted via the internet to **Semper Vivo's** servers. **Semper Vivo** acts as a data repository for your encrypted data. Semper Vivo has no knowledge of means of knowing what the data says. **Semper Vivo's** customers are the only ones in possession of the decryption key to their data. **Semper Vivo** has no way to access the "individually identifiable health information" data, no knowledge of the data and no ability to distribute the data in any way.

**Semper Vivo** will enter into enter into a chain of trust partner agreement as required by HIPAA. This contract states the parties agree to electronically exchange data and to protect the transmitted data. The sender and receiver of data are required and depend upon each other to maintain the integrity and confidentiality of the transmitted information.

Privacy regulations were released in December 2000. They were made final on April 14, 2001, and went into effect in April 2003. Initial compliance date for security measures to be implemented is April 20, 2005 (Title 45 § 164.318).

HIPAA Requirements	SEMPER VIVO Service
Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. <b>§ 164.306</b>	Access is restricted by password authentication to ensure only authorized individuals have access to the data.
Protect against any reasonably anticipated uses or disclosures of such information that are not permitted. <b>§ 164.306</b>	The data is encrypted before transmission and is transferred via a secure virtual private network.
Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. <b>§ 164.306</b>	SEMPER VIVO services include anti virus, anti spam, anti phishing, and protect you from malware. Any intrusions or incidences are immediately identified and reported. Additionally, through SEMPER VIVO's redundancy network, the data is protected from geological, meteorological and natural disaster or political threats.
Implement policies and procedures to prevent, detect, contain, and correct security violations. <b>§ 164.308</b>	SEMPER VIVO has a detection system to identify any attempts at unauthorized access of the data. Our systems are monitored 24/7/365. Any security threats are immediately handled by interrupting access to the data.  SEMPER VIVO maintains audit logs, access reports and security incident tracking reports.
Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information. <b>§ 164.308</b>	Together we will establish user access guidelines, level of access, and implement strong password protection.  All access is date and time stamped by user providing a clear audit trail.
Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends. <b>§ 164.308</b>	SEMPER VIVO provides you with immediate access to terminate user permissions to access the data.
Perform periodic security updates. <b>§ 164.308</b>	SEMPER VIVO services ensure that security measures are constantly being updated so that you don't have to worry.
<i>Protection from malicious software</i> – Implement procedures for guarding against, detecting, and reporting malicious software. <b>§ 164.308</b>	SEMPER VIVO services include anti virus, anti spam, anti phishing, and protect you from malware. Any intrusions or incidences are immediately identified and reported.
<i>Log-in monitoring</i> – Implementation of procedures for monitoring log-in attempts and reporting discrepancies. <b>§ 164.308</b>	SEMPER VIVO maintains a log of all activities regarding log-in attempts. We identify unauthorized log-in attempts and block them.
<i>Password management</i> - Procedures for creating, changing, and safeguarding passwords. <b>§ 164.308</b>	SEMPER VIVO requires the use of strong passwords and uses 128-bit encryption. Passwords can only be reset by the administrator or through an email back to the user who requested the password be reset.

HIPAA Requirements	SEMPER VIVO Service
<p><i>Contingency plan</i> - Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. <b>§ 164.308</b></p>	<p>In case of an emergency such as the destruction of your facility, your data is safe at SEMPER VIVO. You can connect to the data via any computer using a VPN and your identification information.</p> <p>SEMPER VIVO's data center is a level 1 secure center. In case our facility is damaged, redundant systems are available at an alternate facility to enable business continuity.</p>
<p><i>Disaster recovery plan</i> - Establish (and implement as needed) procedures to restore any loss of data. <b>§ 164.308</b></p>	<p>Should your data be lost at your desktop level, any data backed up to the server can be instantly mirrored to another available desktop unit by connecting the new unit via VPN to the network and recreating the lost desktop.</p> <p>At the server level, our systems are configured for automatic fail-over. Redundant servers are standing by to automatically replace any systems that fail.</p>
<p><i>Emergency mode operation plan</i> - Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. <b>§ 164.308</b></p>	<p>In emergency mode, you are ensured business continuity with SEMPER VIVO's services. Should you suffer the loss of a desktop unit, simply replace it and we will mirror the lost unit. Your data is accessible from any where from any computer as long as you have your password and a VPN link.</p>
<p><i>Emergency access procedure</i> - Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. <b>§ 164.316</b></p>	<p>In case of internet failure, a resident copy of all data backed up in the server is available on the computer that was backed up to the server.</p>
<p><i>Data backup plan</i> - Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information. <b>§ 164.308</b></p>	<p>SEMPER VIVO has a redundant fail-safe system to protect that data during backups and storage. The data is housed in a primary data center and a secondary copy is housed offsite.</p>
<p><i>Facility access controls</i>. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. <b>§ 164.310</b></p>	<p>SEMPER VIVO secures physical access to their data center by a) providing access to the data center only to the employees that work directly with the equipment; b) not disclosing the location of the facility to the general public or its workers unless they work at the facility; c) by having 24/7 recordings of traffic inside and outside the facility; d) through the use of a badge to gain access to the facility; and e) any necessary contractor/visitor to the data center must sign in and their activities are monitored and recorded.</p>
<p>Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored. <b>§ 164.310</b></p>	<p>SEMPER VIVO has policies and procedures in place to ensure proper disposition of all electronic protected health information and the hardware or electronic media upon which it is stored.</p>

HIPAA Requirements	SEMPER VIVO Service
<p><i>Media re-use</i> - Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.  <b>§ 164.310</b></p>	<p>Media will be scrubbed and tested to ensure the removal of all records before the media is available for re-use.</p>
<p><i>Unique user identification</i> - Assign a unique name and/or number for identifying and tracking user identity.  <b>§ 164.312</b></p>	<p>Each user is assigned a unique ID and strong password to identify them and track their access of the data and the system.</p>
<p><i>Automatic logoff</i> - Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. <b>§ 164.316</b></p>	<p>Users who are logged into the system and become inactive are automatically logged off after the predetermine time frame established by the client.</p>
<p><i>Encryption and decryption</i> - Implement a mechanism to encrypt and decrypt electronic protected health information.  <b>§ 164.316</b></p>	<p>Data will be encrypted prior to transfer over a secure VPN. A decryption key will reside at each the client's site and with Semper Vivo.</p>
<p><i>Transmission security</i>. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. <b>§ 164.316</b></p>	
<p><i>Integrity</i>. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. <b>§ 164.316</b></p>	<p>Providing IDs and passwords to users and date-time stamping access helps ensure integrity of the data. Backup systems ensure that any data that is improperly altered or destroyed can be retrieved.</p>
<p>Retain the documentation for 6 years from the date of its creation or the date when it last was in effect, whichever is later.  <b>§ 164.316</b></p>	<p>SEMPER VIVO 's system provides for storage of documentation for the preset time limit. Automatic procedures are set in place for the immediate disposal of the records upon expiration of the designated time frame.</p>
<p>If the data is processed through a third party, entities are required to enter into a chain of trust partner agreement</p>	<p>SEMPER VIVO will enter into a Business Associate Agreement in which the parties agree to electronically exchange data and to protect the transmitted data. The Agreement states that the receiver of data (Semper Vivo) is required to maintain the integrity and confidentiality of the transmitted information.</p>

## Title 45 § 164.304 Definitions

*Access* means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

*Administrative safeguards* are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

*Authentication* means the corroboration that a person is the one claimed.

*Availability* means the property that data or information is accessible and useable upon demand by an authorized person.

*Confidentiality* means the property that data or information is not made available or disclosed to unauthorized persons or processes.

*Encryption* means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

*Facility* means the physical premises and the interior and exterior of a building(s).

*Information system* means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

*Integrity* means the property that data or information have not been altered or destroyed in an unauthorized manner.

*Malicious software* means software, for example, a virus, designed to damage or disrupt a system.

*Password* means confidential authentication information composed of a string of characters.

*Physical safeguards* are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

*Security or Security measures* encompass all of the administrative, physical, and technical safeguards in an information system.

*Security incident* means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

*Technical safeguards* means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

*User* means a person or entity with authorized access.

*Workstation* means an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.