atlantic.net
Secure Cloud Services

CELEBRATING 29 YEARS OF EXCELLENCE

WHAT MAKES ATLANTIC.NET HIPAA COMPLIANT?

Atlantic.Net is a leading business in healthcare hosting; HIPAA Compliant Hosting is one of our most successful on-demand services. Atlantic.Net complies with the required physical, technical, and administrative safeguards of HIPAA, and we offer a principal platform for our healthcare partners to become HIPAA-ready in no time.

Our teams are audited at least once a year to ensure that we adhere to the mandatory best practices, business processes, and safeguarding measures needed to protect the integrity of electronic Protected Health Information (ePHI).

In reality, the checks and balances Atlantic.Net uphold far exceed the minimum requirements for HIPAA compliance. We always aim to go above and beyond to secure our healthcare clients' cloud data. The company provides extensive managed services, managed security, and high-end encryption, and fully complies with SOC 2 and SOC3. Furthermore, Atlantic.Net is fully compliant and audited against the demanding HIPAA and HITECH standards.

WHAT IS HIPAA?

HIPAA is a Health Insurance Portability and Accountability Act that was signed and enacted into law on August 21, 1996. The law was created to uphold the data integrity of protected health information (PHI) and offer guarantees to patients about how their data was handled.

IS ATLANTIC.NET HIPAA COMPLIANT?

Absolutely yes for our in-scope HIPAA-Compliant Hosting! As a business, we thrive and excel giving our customers the best HIPAA platform for their needs. For clarity, we provide other (non-HIPAA-Compliant) hosting services in-house, and you will find all HIPAA-Complaint services on our main page.

WHAT MAKES ATLANTIC.NET HIPAA COMPLIANT?

In this article, we will examine what responsibilities belong to Atlantic.Net, what responsibilities our healthcare customers have, and what responsibilities are shared between Atlantic.Net and our customers.

atlantic.net
Secure Cloud Services

CELEBRATING 29 YEARS OF EXCELLENCE

WHAT MAKES ATLANTIC.NET HIPAA COMPLIANT?

WHAT IS ATLANTIC.NET RESPONSIBLE FOR?

- **Cloud Servers** - Atlantic.Net manages the entire HIPAA compliant stack, including the servers, networking, and storage. This management includes support and maintenance on all proprietary cloud software.
- **Storage** - The maintenance and upgrades of the storage platform are the sole responsibility of Atlantic.Net. We will ensure the performance of the storage is always excellent and we will continue to improve and upgrade our storage to exceed industry needs. Our engineers will replace any failed disks within an agreed SLA and destroy the damaged media to HIPAA standards.
- **Networking** - The network layer is controlled and audited by Atlantic.Net. We segregate traffic per HIPAA regulations and operate a continuous upgrade program to ensure the infrastructure is protected to the highest standards.
- **Encryption at Rest** - Safeguarding PHI is our number one priority, and we provide encryption at rest on all Atlantic.Net Cloud platforms by default. The storage layer is protected by a minimum of AES256 encryption, and only Atlantic.Net has the private key to access and unlock the at-rest data.
- **Physical Security** - Our servers are located in highly secure data center compounds that are protected by access control systems. Physical access to and from the server room is limited to very few essential employees, and the building and premises are monitored by CCTV and security personnel 24x7.
- **Data Center** - We provide a 100% uptime guarantee with our Service Level Agreement. We do this by having our data centers configured in a way to allow co-maintainability along with the ability to lose any one point of failure without causing any physical data center issues for the power, cooling, and networking.

WHAT IS THE HEALTHCARE CUSTOMER RESPONSIBLE FOR?

Atlantic.Net will do as much as possible to help our healthcare clients. We are always available for help and assistance, so do not hesitate to get in touch.

- **Database** - Clients are responsible for the day-to-day maintenance of any database applications hosted on the platform, including database security, user credentials, and privileges. This also includes the data contained within the database. If the customer requires the database to be additionally encrypted, this must be managed by the customer; this is highly recommended according to industry best practices.
- **Customer Data** - The customer is solely responsible for client data. Atlantic.Net has no access to any of the data files on your service, so it is the customer's responsibility to ensure PHI is encrypted and that customer records are correct.
- **Applications** - It is the customer's responsibility to manage and maintain any additional software and licenses used in day-to-day operations, including off-the-shelf applications or in-house custom software. Identity and Access Management - The client has ownership of the entire user lifecycle. Atlantic.Net provides the tools to complete the job; however, the customer must add, modify and delete users and handle all access queries including permissions.

WHAT MAKES ATLANTIC.NET HIPAA COMPLIANT?

- **Client-side data encryption and data integrity authentication** - Any frontend client-side encryption technology, such as PGP, BitLocker, and application-specific encryption, is the responsibility of the customer.
- **Service-Side Encryption (File System and/or Data)** - Any backend service-side encryption technology, typically database and application-specific encryption, is the responsibility of the customer outside of the physical disks, since they are encrypted at rest by default by ACP.

WHAT ARE THE SHARED RESPONSIBILITIES BETWEEN ATLANTIC.NET AND OUR HEALTHCARE CUSTOMERS?

Making HIPAA compliance work requires the creation of a shared responsibility matrix. Both parties have a joint responsibility to meet the compliance goals set out in HIPAA legislation.

- **Operating System** - Atlantic.Net is responsible for the hardware layer firmware levels of the compute nodes, networking, and storage. This also includes patching and maintenance of the hypervisor of the cloud platform. The customer is responsible for the base operating system such as Windows Updates or Yum Updates for Linux, including scheduling. Customers can also opt for a managed service offering that includes patch management performed by our technical teams.
- **Firewall** - A Fully Managed Firewall service is provided and maintained by Atlantic.Net for managed services customers. We ensure the availability and privacy of the service. Self-service customers can utilize the operating system's built-in firewall features or another avenue that best fits their needs if they do not opt for the Fully Managed Firewall.
- **VPN** - For managed services customers taking the Managed Firewall option, we offer a VPN service to secure and encrypt a point-to-point tunnel for end-users. Atlantic.Net maintains the hardware and software that provides this connectivity, but the customer must enforce its use and manage user activity over the VPN.
- **Backup** - Our highly redundant backup service is available to all our HIPAA clients. The service can be configured for Onsite and Offsite backups. It is the customers' responsibility to ensure that the backup services meet or exceed the requirements of the customer's business. An enhanced replication service is available on request; please contact our sales team for more information
- **Intrusion Prevention Service** - The IPS scans the network layer and sniffs for unusual activity. Atlantic.Net offers this as a fully managed service, and this IPS provides insights into who is trying what on your network along with your Fully Managed Firewall.
- **Trend Micro™ DEEP SECURITY System Security Package** - By monitoring critical operating system and application files, such as directories, registry keys, and values, Integrity Monitoring detects and reports malicious and unexpected changes to files, the hypervisor, and systems registry in real-time. Log inspection optimizes the identification of key security events buried in log files across the data center, which the SIEM system correlates, reports, and archives. Event tagging replicates actions for similar events across the entire data center, reducing cost, while agentless configuration adds security to virtual machines without adding footprint.

atlantic.net
Secure Cloud Services

CELEBRATING 29 YEARS OF EXCELLENCE

WHAT MAKES ATLANTIC.NET HIPAA COMPLIANT?

- **Integrity Monitoring** - The cloud monitoring service provides numerous real-time performance stats regarding the customers' infrastructure. The customer is responsible for reacting to identified issues that might be caused by bad actors or malicious software.
- **Anti-Malware** - Malware is a serious concern for anyone with a cloud presence. Atlantic.Net provides new cloud servers that are free from malware, but we recommend our customers have anti-malware software installed and updated. Not all anti-malware will be suitable, so picking one of the best in the market and ensuring constant updates is a key part of HIPAA compliance.
- **DNS** - Atlantic.Net hosts a highly efficient DNS platform to manage how your domain names interact with the HIPAA compliant hosting platform. Configuration of the platform is down to the individual customer, as well as managing domain name purchases and maintenance. If you have any issues, Atlantic.Net is here to help with our Managed Services division.
- **Multi-Factor Authentication (MFA)** - MFA is a very effective way to reduce the attack surface of a healthcare customer. Token-based access is defined using either a local app or mobile phone. Atlantic.Net manages the infrastructure that provides the service, and the customer looks after user management, key management, and device management, including the revoking of user access.
- **Web DDoS Protection** - The DDoS managed service is a highly efficient platform for automatically detecting unexpected traffic spikes or DDoS attacks. The service is managed by Atlantic.Net, but we appreciate feedback and interaction with our clients, as sometimes the customer notices something is amiss first. A content delivery network (CDN) improves protection further and delivers significant performance boosts to high traffic customers. The CDN platform is managed by Atlantic.Net, but the customer has to ensure that no PHI is cached on the CDN.
- **Vulnerability Scanning** - Atlantic.Net offers vulnerability scans as part of our Managed Server offering. This service will scan your entire environment while looking for any possible vulnerabilities that may be present. If you have the Managed Server offering, we will work hand in hand with you and your team to ensure these holes are patched.

As you can see, Atlantic.Net introduces several safeguards and standards needed to uphold HIPAA compliance. The service is durable and security-conscious and, working together with our healthcare customers, the platform has evolved and will continue to grow as our customer needs change.

Ready to Find Out More?

For over 25 years, Atlantic.Net has helped thousands of businesses with industry-leading HIPAA compliant cloud hosting solutions. Atlantic.Net Cloud is a far superior alternative to traditional providers, providing full control of your cloud server hosting software backed by either public or dedicated resources. Contact an advisor at 888-618-3282 or email us at sales@atlantic.net to get started with a hosting solution for your business!