



DATA PRIVACY

FOR VIRTUAL MAILBOXES:

How VPM ensures SOC 2 and HIPAA compliance

Safeguard confidential data with VPM's mail management solutions

www.virtualpostmail.com



Table of Content

01

Introduction

03

How VPM meets
SOC 2 standards across
virtual mailbox services

04

VPM's commitment
to HIPAA compliance

Introduction

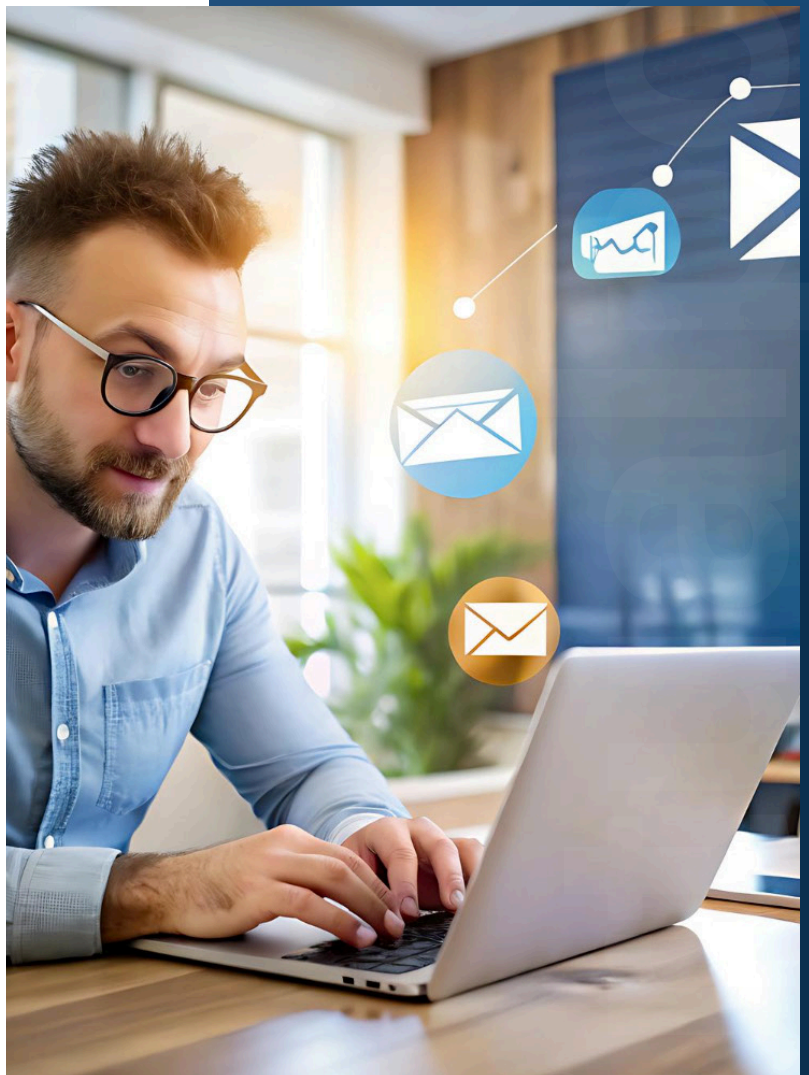
In 2023, the **global average cost of a data breach soared to \$4.45 million**, underscoring the urgent need for companies to address the rising threat of cyberattacks. As the reliance on digital communications grows, the risks of identity theft, data breaches, and privacy violations are increasing, making the implementation of strong security measures more critical than ever.

In just the past year alone, **725 healthcare data breaches were reported to the Office for Civil Rights**, with more than 133 million records exposed or impermissibly disclosed. Ticketmaster reported a staggering **560 million customer records breached**, which included confidential data like history, payment information, names, and addresses. Even more alarming, genetic company 23andme was impacted by a data breach resulting in the release of **several thousand customers' private genetic data**.

VPM fully understands the importance of preventing catastrophic data breaches and ensuring secure digital mail services for each and every customer. Safeguarding your sensitive data is, and will always be, at the forefront of the company's mission.

In this white paper, we'll examine VPM's security measures in greater detail. Key findings include:

- VPM ensures the highest level of data security by adhering to both SOC 2 Type II and HIPAA standards, providing solid protection for sensitive information.
- As an added assurance, VPM can sign a Business Associate Agreement, further reinforcing our commitment to protecting healthcare-related data.
- Continuous monitoring, regular audits, and advanced encryption methods are integral to VPM's approach, safeguarding data at every stage of its lifecycle.
- With secure facilities and 24/7 surveillance, VPM offers robust physical security to complement its digital protections.



The essential role of HIPAA and SOC 2 certifications in healthcare

For healthcare providers, safeguarding sensitive patient information is of the utmost importance. Health Insurance Portability and Accountability Act (HIPAA) and System and Organization Controls 2 (SOC 2) certifications play a vital role in ensuring that healthcare organizations meet stringent data protection and privacy standards.

HIPAA compliance is fundamental for any healthcare-related service that handles protected health information (PHI). It ensures that virtual mailbox services adhere to strict privacy and security rules designed to protect patient data from unauthorized access and breaches.

For healthcare organizations, having a HIPAA-compliant virtual mailbox means that all sensitive patient information and medical records are securely transmitted and stored. This compliance is not only a legal requirement, but also builds trust with patients who expect their personal health data to be handled with the highest level of confidentiality.

SOC 2 certification provides an additional layer of assurance regarding the operational controls and practices of service providers. It focuses on five key trust service criteria: security, availability, processing integrity, confidentiality, and privacy.

For a healthcare organization using a virtual mailbox service, SOC 2 certification guarantees that the service provider adheres to rigorous standards for protecting data against unauthorized access and ensuring its availability when needed. This certification is crucial for maintaining operational transparency and demonstrating a commitment to high standards of data protection and service reliability.

Together, HIPAA and SOC 2 certifications ensure that virtual mailbox services not only comply with legal requirements, but also operate with the highest standards of security and privacy. For healthcare organizations, leveraging a SOC 2 Type II certified virtual mailbox service mitigates the risks associated with data breaches and compliance failures, providing a secure and reliable solution for managing essential communication and documentation.



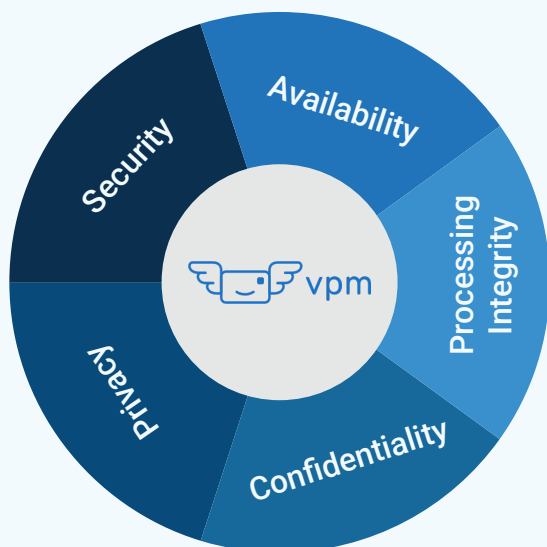
How VPM meets SOC 2 standards across virtual mailbox services

SOC 2 certification involves an intensive audit process that closely monitors an organization's security measures and how they protect customer data.

To achieve SOC 2 certification, companies must develop a cybersecurity program that meets SOC 2 standards, undergo an audit by an AICPA-affiliated CPA, and have their infrastructure and security practices evaluated against the five Trust Services Criteria (TSC): security, privacy, confidentiality, processing integrity, and availability.

VPM meets SOC 2 standards by consistently adhering to these criteria, maintaining strict controls, and security policies to ensure ongoing compliance.

Chart here covering the key principles (security, availability, processing integrity, confidentiality, privacy)



Security

- Network /application firewalls
- Two-factor authentication
- Intrusion detection



Availability

- Performance monitoring
- Disaster recovery
- Security incident handling



Privacy

- Access control
- Two-factor authentication
- Encryption



Processing Integrity

- Quality assurance
- Processing monitoring



Confidentiality

- Encryption
- Access control
- Network/application firewalls

Security

VPM's security measures are designed to protect against unauthorized access, utilizing strategies such as network firewalls, two-factor authentication (2FA), physical security protocols, and secure on-site mail shredding

Network/Application Firewalls

At VPM, we host our entire infrastructure on Amazon Web Service (AWS), which is fully SOC2 and HIPAA compliant. Your data security is prioritized with powerfully built network and application firewalls, including AWS Network Firewall.

Key features include:

- **VPC (Virtual Private Cloud):** Allows isolation of network resources with custom IP ranges, subnets, and route tables.
- **Security Groups:** Acts as virtual firewalls for instances, controlling inbound and outbound traffic at the instance level.
- **Network ACLs:** Provides additional stateless filtering of traffic for subnets, controlling traffic flow at the subnet level.
- **AWS Shield:** Provides DDoS protection to ensure availability and resilience of the network.

- **AWS WAF (Web Application Firewall):** Protects web applications from common exploits such as SQL injection and cross-site scripting (XSS).
- **Traffic Encryption:** End-to-end encryption for data in transit using protocols such as TLS to protect the confidentiality and integrity of network communications.
- **VPC Flow Logs:** Enables network traffic monitoring to capture and analyze IP traffic patterns for security audits and anomaly detection.
- **IAM Policies and Roles:** Controls access to network and firewall resources, ensuring only authorized users can configure or access the infrastructure.

Together, these components help maintain the security, availability, and integrity of network communications in compliance with SOC 2.

Two-Factor Authentication (2FA)

Two-factor authentication (2FA) is a critical element of VPM's security strategy, offering protection against phishing, social engineering, and password brute-force attacks. 2FA is a foundational component of a zero-trust security model, which requires strict verification of users attempting to access sensitive data.

VPM implements 2FA for customer accounts, requiring an additional verification step beyond the standard username and password.

Physical Security Protocols

To prevent unauthorized access or tampering with mail items, VPM has a designated system of protocols in place. All physical locations are equipped with advanced security controls, including round-the-clock surveillance systems, controlled access, and alarm systems to protect physical mail and data storage areas from unauthorized access and potential security breaches.

On-site Mail Shredding

For the disposal of sensitive information, all physical mail is securely shredded on-site using a certified mobile shredding service. This process ensures that mail never leaves our facility for destruction, reducing the risk of unauthorized access. Shredding occurs directly on our premises, providing an additional layer of security and peace of mind.

By employing this secure method, we ensure that sensitive information is properly disposed of, maintaining the integrity and privacy of our clients' communications. This minimizes the risk of data exposure by ensuring that all discarded materials are irreversibly destroyed. Document destruction certificates are available upon request.



Availability

VPM's commitment to availability encompasses performance monitoring, incident response, and breach notification. These actions ensure that our services are consistently operational and accessible, minimizing downtime and maintaining full customer trust.

Performance Monitoring

VPM employs comprehensive performance monitoring, which involves using advanced monitoring tools to track system performance and availability in real time. This helps to identify and address potential issues before they impact customers. Additionally, VPM analyzes usage patterns and trends to anticipate future needs and scale infrastructure accordingly, ensuring that services can handle increased demand without degradation in performance.

Incident Response

To maintain high availability, VPM has established protocols for quickly responding to and managing security incidents or breaches. By rapidly detecting potential incidents through continuous monitoring and automated alerts, affected systems can be isolated and impact mitigated. Should a breach be detected, VPM will conduct a thorough investigation to determine the cause as well as implement corrective actions to resolve the incident and restore normal operations.

Breach Notification

In the event of a data breach involving customer information, VPM is committed to notifying affected customers within the legally allowed time after confirming the breach. This includes utilizing data forensics to assess and confirm the data breach, determine its extent, and provide detailed information about the breach, including what happened, what information was affected, and the steps VPM is taking to address the breach and prevent future incidents.



Processing integrity

VPM is dedicated to ensuring the highest standards of processing integrity, focusing on the completeness, validity, accuracy, timeliness, and authorization of system and information processing. This commitment involves due diligence, continuous monitoring, regular audits, and maintaining transparency with customers.

Due Diligence

VPM enforces stringent security controls through due diligence measures, requiring subprocessors to enter into agreements that mandate adherence to SOC 2 principles. Each subprocessor undergoes a comprehensive evaluation to ensure they can adequately protect customer data and adhere to high security and privacy standards, consistent with SOC 2 principles. In addition, subprocessors must report any breaches or security incidents promptly, allowing VPM to take necessary actions to mitigate potential impacts.

Continuous Monitoring

At VPM, continuous monitoring is a key element of our security strategy, ensuring both system integrity and the protection of customer data. This proactive approach allows us to quickly detect any deviations from security standards and immediately address potential threats. We also have a comprehensive incident response plan in place to swiftly handle and mitigate any security issues, minimizing potential impacts on our customers.

Regular Security Audits

VPM conducts regular security audits to verify compliance with internal policies and external regulatory requirements, as well as identify potential vulnerabilities and areas for improvement. These audits involve ensuring that all practices align with VPM's privacy notice as well as Generally Accepted Privacy Principles (GAPP), maintaining adherence to the highest level of standards. We also maintain detailed logs of all subprocessor activities and regularly review these to ensure accountability.

Maintaining Data Transparency

VPM is dedicated to providing transparency and assurance to its customers regarding how your data is used. Barring a subpoena or court order, your data is never sold, rented, or provided to third parties unless you grant them permission. Customers may request an up-to-date list of subprocessors, including their roles and the types of data they process.



Confidentiality

VPM is deeply devoted to protecting confidential information from unauthorized disclosure. This commitment involves employing advanced encryption techniques, stringent access controls, and robust password management practices to ensure the security and confidentiality of customer data.

Bank-level Data Encryption at Rest

Mail data is securely stored on AWS S3, with encryption at rest using the AES-256 encryption standard, managed through AWS Key Management Service (KMS). This robust encryption ensures data confidentiality and integrity while stored on our systems. VPM uses AES-256 encryption—commonly referred to as "bank-level" encryption. This encryption standard is among the most secure available and is used to encrypt billing data. When your payment information is processed and stored, it is encrypted and managed within PCI-DSS compliant systems. This ensures that your credit card information is securely protected from unauthorized access, fraud, and theft.

Comprehensive Encryption for Data in Transit

Data encryption is not limited to storage; it also encompasses data in transit. VPM utilizes SSL/TLS certificates to encrypt data as it moves between your device and our servers. For sites and applications hosted on AWS, we rely on SSL certificates generated by AWS certificates issued by AWS Certificate Manager (ACM) to secure all sites and applications hosted on AWS. This encryption is essential for protecting data in flight, ensuring that it remains confidential and intact as it travels across the internet.

Additionally, our customer portal, hosted on Netlify, uses Netlify's own SSL certificate system to secure user interactions with the portal. For sites fronted by Cloudflare, we leverage Cloudflare's certificate system, which further enhances the security of data in transit by providing SSL encryption.



Privacy

VPM is dedicated to ensuring that personal information is collected, used, retained, disclosed, and disposed of in accordance with the organization's privacy notice and the AICPA's generally accepted privacy principles (GAPP). This commitment involves the implementation of role-based access control and comprehensive logging to uphold the highest standards of privacy protection.

Access Controls

Access to customer data at VPM is tightly controlled to ensure that only authorized personnel can access sensitive information. Access levels are commensurate with job responsibilities, ensuring that higher levels of access are limited to those who require it. To minimize the risk of unauthorized access by former employees, access is disabled within one business day following an employee's termination.

Access to production data is strictly controlled to only production-level systems admin, audited, and logged to a separate AWS security account purely for storing audit logs and cannot be altered or deleted (append-only).

Comprehensive Logging

To ensure transparency and accountability, VPM maintains detailed logs of all activities related to the handling of customer mail and data. These detailed logs create an audit trail that is essential for tracking and auditing purposes, ensuring that any unauthorized access or anomalies can be promptly identified and addressed. It also helps maintain compliance with privacy policies and regulatory requirements.

VPM's commitment to HIPAA compliance

HIPAA compliance plays a critical role in safeguarding sensitive patient information. Unlike traditional postal services, which are exempt from HIPAA regulations under the conduit exception, virtual mailbox services are considered business associates of covered entities. Because these services may have access to clients' Protected Health Information (PHI), it is essential for virtual mailbox providers to adhere to HIPAA compliance standards. This ensures the confidentiality, integrity, and security of the PHI they may encounter.

At VPM, we implement a range of safeguards to protect PHI and maintain full compliance with HIPAA regulations. Our security measures address the Privacy Rule, Security Rule, Breach Notification Rule, and Omnibus Rule to ensure comprehensive protection.

The Privacy Rule

The HIPAA Privacy Rule sets national standards to protect individuals' medical records and other protected health information, otherwise known as PHI.

VPM strictly adheres to the HIPAA Privacy Rule by ensuring that PHI is used and disclosed only for authorized purposes, with safeguards in place to protect patients' privacy rights and limit access to the minimum necessary information.



Advanced Data Encryption at Rest

To safeguard your sensitive payment details, VPM employs AES-256 encryption, often known as "bank-level" encryption. This highly secure standard protects your billing data by encrypting it during processing and storage. Our systems comply with PCI-DSS standards, ensuring your credit card information remains secure against unauthorized access, fraud, and theft.

Encryption in Transit

All communications between customers and VPM's services are encrypted, ensuring that sensitive information, such as scanned mail images and personal data, is protected from interception. To protect sensitive information during transmission, VPM employs Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocols. SSL and TLS protocols provide data integrity, ensuring that information sent between VPM and its customers is not tampered with during transmission.

Role-based Access Controls (RBAC)

VPM uses Role-Based Access Controls (RBAC) to regulate PHI access, ensuring personnel only access the information necessary for their job functions. Access is strictly limited to authorized individuals managing systems containing PHI.



The Security Rule

VPM complies with the a by implementing stringent safeguards to protect the confidentiality, integrity, and availability of PHI. This includes physical, technical, and administrative measures to prevent unauthorized access and ensure data security.

On-site Alarm and Security Systems

In addition to maintaining secure facilities equipped with 24/7 surveillance, VPM employs continuous monitoring that ensures only authorized personnel can access sensitive areas. The combination of physical security measures and advanced surveillance technology ensures the highest level of safety for PHI.

Regular Security Audits

VPM conducts regular security audits to maintain HIPAA compliance, identifying and addressing system vulnerabilities and ensuring subprocessors meet VPM's strict security standards.

Comprehensive Logging

VPM keeps detailed logs of all access and actions on systems containing PHI, recording who accessed data, what actions were taken, and when. These logs are essential for ongoing monitoring and auditing, allowing quick detection and response to potential security incidents.

The Breach Notification Rule

VPM adheres to the HIPAA Breach Notification Rule by promptly addressing any security incidents involving PHI. In the event of a breach, we are committed to investigating, mitigating, and notifying affected customers within the required timeframe, ensuring transparency and compliance with regulatory obligations.

Incident Response Plan

VPM has a structured incident response plan to handle and mitigate security breaches involving PHI. This plan includes procedures for containing and investigating breaches. In the event of a breach, VPM will notify customers within 30 days to ensure prompt action to protect affected individuals and comply with regulatory requirements.



The Omnibus Rule

The Omnibus Rule, enacted in 2013, significantly expanded the scope and requirements for Business Associate Agreements (BAAs).

It mandated that business associates, in addition to covered entities, must be HIPAA compliant.. It also requires that BAAs be executed between a covered entity and business associate, or between two business associates, before any PHI or ePHI can be shared.

BAAs are now a critical component of HIPAA compliance, ensuring that all entities handling PHI are held to appropriate standards of privacy and security. VPM fully complies with the HIPAA Omnibus Rule by extending HIPAA obligations to all business associates and subcontractors.

Business Associate Agreement

A business partner is considered a Business Associate if it creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA. VPM is committed to maintaining HIPAA compliance and will sign Business Associate Agreements with organizations to formalize this commitment. These agreements outline VPM's responsibilities in protecting PHI and ensure compliance with HIPAA regulations.

It's important to note that while many mail services claim to comply with HIPAA regulations, true HIPAA compliance requires more than a simple commitment. Unless a provider offers Business Associate Agreements (BAAs)—and many do not—they are not fully compliant. VPM, however, provides BAAs to ensure that our services meet the highest standards of HIPAA compliance, giving you full confidence that your protected health information (PHI) is secure.

Conclusion

In today's digital era, ensuring the security of sensitive information is more important than ever. As cyber threats continue to grow and impact consumers, choosing a mail handling provider that prioritizes security measures is essential. VPM stands out as a trusted partner for individuals and businesses seeking a secure, reliable virtual mailbox solution.

With strict adherence to SOC 2 standards and full HIPAA compliance, VPM safeguards every aspect of your mail management. Through advanced encryption, comprehensive access controls, continuous monitoring, and secure on-site processing, VPM provides exceptional protection for your data. These rigorous measures not only defend against potential threats, but also guarantee that your information is handled with the highest level of care and integrity.

When it comes to safeguarding your sensitive information, don't take unnecessary risks. Choose VPM for your virtual mailbox needs and benefit from an unmatched level of security and compliance. Sign up with VPM today and take the first step toward securing your mail and confidential data with a partner you can trust.





THANK YOU!

www.virtualpostmail.com

