venn

WHITE PAPER

HIPAA Compliance

How Companies can Meet Healthcare Compliance Requirements with Venn

HIPAA Compliance: How Companies can Meet Healthcare Compliance Requirements with Venn

HIPAA compliance safeguards the privacy and security of protected health information (PHI). It ensures that healthcare providers, insurers and other entities handling sensitive health data implement appropriate measures to prevent unauthorized access, breaches and misuse. When it comes to connectivity and security systems, these solutions must protect the integrity and confidentiality of PHI within the system.

Venn has meticulously aligned its policies and procedures with HIPAA's administrative, physical, and technical safeguards to comply with these standards comprehensively.

In the following whitepaper, we detail which policies and procedures Venn has taken upon itself to meet HIPAA requirements. This report provides a bird's eye view, but you can find additional details, procedures and explanations, as well as a map to HIPAA criteria, by contacting us at venn.com/contact-us.

Table of Contents

- ADMINISTRATIVE SAFEGUARDS 5
- PHYSICAL SAFEGUARDS 7
- TECHNICAL SAFEGUARDS 8
- POLICIES, PROCEDURES AND DOCUMENTATION 9
- OUR COMMITMENT 10

Administrative Safeguards

Security Management Process

Venn implements a robust information security management system with over 50 controlled policies, procedures and standards aimed at preventing, detecting, containing and correcting security violations. Internal reviews, incident response processes, and risk management programs ensure ongoing compliance and improvement.

Assigned Security Responsibility

The Chief Technology Officer and VP Information Security and Compliance are tasked with overseeing the development and implementation of security policies, procedures and compliance.

Workforce Security

Job descriptions, background checks and approved roles based on least privilege principles ensure that only authorized personnel access sensitive information. Procedures are in place for authorizing, supervising, and terminating workforce access.

Information Access Management

Policies for authorizing access, establishing, and modifying access rights are in place. Regular user access reviews and the management of user accounts are rigorously enforced.

Security Awareness and Training

Continuous training programs, including quarterly security updates, equip employees with the necessary skills and awareness to guard against threats such as malicious software.

Security Incident Procedures

A structured incident response policy enables effective responses to security incidents, documenting and mitigating harmful effects while informing management regularly.

Contingency Plan

Comprehensive contingency planning, including data backup, disaster recovery, and emergency mode operation plans, ensures protection of sensitive systems, network devices, applications, and data during emergencies. Regular testing and updates of these plans are conducted.

Evaluation

Regular internal and external assessments, including vulnerability tests, penetration tests and phishing tests, help evaluate the effectiveness of Venn's security controls.

Business Associate Contracts

Venn performs risk assessments of high-risk vendors and maintains Business Associate Agreements to ensure that subcontractors also adhere to HIPAA standards.

Physical Safeguards

Facility Access Controls

Policies limit physical access to data centers, ensuring only authorized personnel have access. Regular reviews and contingency procedures support data restoration efforts.

Workstation Use and Security

Policies specify the correct use and security of workstations, based on least privileges and the segregation of duties. Venn management authorizes and approves access and privileged access.

Device and Media Controls

Procedures govern the receipt, removal, and disposal of hardware and electronic media, ensuring data is rendered unreadable before disposal. Venn customer files are backed up, retained, and replicated in accordance with customer contracts.

Technical Safeguards

Access Control

Venn uses multi-factor authentication (MFA) and single sign-on (SSO) to secure access to systems. Unique user IDs and session termination policies enhance accountability and security.

Audit Controls

Regular audits, including external penetration tests and vulnerability scans, monitor and examine system activity to detect and respond to anomalies.

Integrity

Measures to protect data from improper alteration or destruction include risk acceptance forms and activity logs with anomaly detection alerts.

Person or Entity Authentication

Procedures ensure that only authorized persons or entities access sensitive applications and systems, verified through MFA and stringent user account management.

Transmission Security

Encryption of VPN traffic, MDA and regular scans of externally-facing devices and logs protect against unauthorized access.

Policies, Procedures and Documentation

Policies, Procedures and Documentation

Venn maintains comprehensive documentation of its policies and procedures, ensuring they are available to relevant personnel and updated in response to environmental or operational changes. Customer information is not disclosed. Venn's documented risk management and assessment program includes ePHI.

Our Commitment

Venn's commitment to HIPAA compliance is evident in our thorough approach to administrative, physical, technical and documentary safeguards. By continuously assessing and updating our policies and procedures, Venn ensures the highest level of protection for sensitive data, maintaining trust and security in the healthcare industry.

About Venn

Venn is revolutionizing BYOD workforces with the first purpose-built, patented technology for securing contractors and remote workers on personal or unmanaged devices. Venn enables security and compliance-driven organizations to eliminate the costs and complexities associated with buying, securing, and managing laptops or dealing with virtual desktops. Similar to an MDM solution but for laptops – work lives in a company-controlled Secure Enclave installed on the user's PC or Mac, where business activity is isolated and protected from any personal use on the same computer. Over 700 organizations, including Fidelity, Guardian, and Voya, trust Venn to meet FINRA, SEC, NAIC, and SOC 2 standards.

Learn more at venn.com.