*Vita*Nexus

Life. Connected.

Data and Security Policy

Effective Date: June 11, 2026
Version 1.0

VitaNexus, Inc. — vitanexus.ai

VITANEXUS

WELLNESS & SOCIAL STORYTELLING

Data and Security Policy

Effective Date: June 11, 2026

Last Updated: June 11, 2026

Document Version: 1.0

This policy governs data collection, storage, security, and user rights for the VitaNexus consumer wellness and social storytelling application. It applies to all platforms including iOS and Android.

⚠ Important Disclaimers — Please Read Before Continuing

NOT A MEDICAL DEVICE / NOT CLINICAL DATA. VitaNexus is a **consumer wellness and social storytelling application only**. Data collected through VitaNexus is wellness and lifestyle data. It is not clinical health data, not Protected Health Information (PHI), and not medical records of any kind. VitaNexus is **not a HIPAA-covered entity** and does not operate under HIPAA's regulatory framework. Do not use VitaNexus to store, manage, transmit, or act upon clinical health information of any kind.

NOT A SUBSTITUTE FOR PROFESSIONAL MEDICAL CARE. Wellness data insights, summaries, patterns, and any informational outputs generated by VitaNexus are provided for **personal informational and self-awareness purposes only**. They do not constitute and must not be interpreted as medical advice, clinical diagnosis, clinical recommendations, or a treatment plan of any kind. Always consult a qualified and licensed healthcare professional for medical guidance.

NOT FOR EMERGENCY USE. VitaNexus does **not** provide emergency data monitoring, emergency alerting, or crisis response services of any kind. VitaNexus must not be used in any situation requiring immediate medical attention. **In any medical emergency, call 911 or your local emergency services immediately.**

CONSULT A QUALIFIED PROFESSIONAL. Any patterns, trends, or insights visible in VitaNexus — including but not limited to mood trends, activity summaries, sleep patterns, and goal progress — should be reviewed with a qualified and licensed healthcare professional before taking any medically relevant action based on them.

FTC WELLNESS DISCLAIMER. Wellness data displayed in VitaNexus is provided for personal awareness only. Interpretations of wellness data vary significantly by individual and are **not clinically validated**. VitaNexus makes no representations that its data features, wellness summaries, or insights are medically accurate, complete, or suitable for any clinical purpose.

APP STORE / GOOGLE PLAY NON-MEDICAL DISCLAIMER. VitaNexus is categorized as a **Health & Fitness and Social Networking** application on the Apple App Store and Google Play Store. Its data features are not intended for and must not be used for clinical, diagnostic, or treatment purposes. VitaNexus does not qualify as a medical device under FDA regulations and has not been cleared or approved by the FDA.

TABLE OF CONTENTS

1. Introduction

VitaNexus, Inc. ("**VitaNexus**," "**we**," "**us**," or "**our**") is a Delaware corporation with its principal place of business in Menomonee Falls, Wisconsin. VitaNexus operates a consumer wellness and social storytelling application available on iOS and Android (the "**Application**" or "**App**"). VitaNexus is built to help individuals track personal wellness goals, express themselves through stories and reflections, and connect with a supportive community — all within a privacy-first, consumer-grade platform.

This **Data and Security Policy** (the "**Policy**") explains:

- What data we collect, and why;
- How we store, protect, and retain that data;
- Who we share data with, and under what conditions;
- What rights users have over their data; and
- How we maintain the security of our systems and your information.

1.1 Scope

This Policy applies to all data collected, stored, transmitted, or processed in connection with your use of the VitaNexus Application, our website(s), and any related services we operate. It applies to all users worldwide, including iOS users, Android users, enterprise partners, and any third-party technical reviewers or regulators reviewing our practices.

1.2 Relationship to Other Policies

This Policy should be read together with our **Privacy Policy** and our **Terms and Conditions**, which together govern your use of VitaNexus. In the event of a conflict between this Policy and another document on a data security or data protection matter, this Policy controls.

1.3 Consumer Wellness Nature of All Data

VitaNexus is a **consumer wellness and social storytelling application**. All data collected through VitaNexus is consumer lifestyle and wellness data. **No data collected through VitaNexus constitutes clinical health data, Protected Health Information (PHI), or medical records under any applicable law.** VitaNexus is not a HIPAA-covered entity, is not a healthcare provider, and does not operate as a medical device. These designations are not merely procedural — they reflect the fundamental design and purpose of VitaNexus as a personal wellness companion, not a clinical tool.

> **Note for Enterprise Partners and Regulators**
>
> VitaNexus intentionally does not collect, process, or store Protected Health Information (PHI) or clinical health data. This design choice eliminates HIPAA applicability by architecture, not by waiver.

If your review requires confirmation of HIPAA non-applicability, please contact us at **privacy@vitanexus.ai**.

2. Data We Collect

VitaNexus collects data in several categories, each described below. We collect only what is necessary to provide the Application's features and to maintain security and quality. We do not collect clinical health data, medical records, or Protected Health Information under any circumstance.

A. Account Data

When you create a VitaNexus account, we collect the information necessary to establish and manage your account:

- **Name** (first and last, as provided by you);
- **Email address**;
- **Username** (chosen by you);
- **Password** (stored as a salted cryptographic hash — your plaintext password is never stored or accessible to VitaNexus employees);
- **Profile photo** (optional, uploaded by you).

B. Wellness and Lifestyle Data

VitaNexus allows you to voluntarily record personal wellness information for your own self-reflection and goal tracking. This may include:

- **Mood entries** — self-reported mood ratings and notes;
- **Activity logs** — voluntary records of physical activities you choose to log;
- **Goal records** — personal wellness goals you set and track;
- **Wellness journal entries** — free-text reflections and notes you write;
- **Sleep inputs** — self-reported sleep duration and quality you choose to enter.

> **Critical Designation**
>
> All wellness and lifestyle data listed in Section 2.B is **personal wellness data entered voluntarily by you for your own self-awareness**. It is **NOT** medical records. It is **NOT** clinical data. It is **NOT** Protected Health Information (PHI). It should **NOT** be used for any medical decision-making purpose. VitaNexus treats this data with elevated sensitivity — see Section 11 (Wellness Data — Special Handling).

C. Social and Storytelling Data

VitaNexus is a social storytelling platform. When you use its community features, we collect:

- **Posts and stories** you create and share within the Application;
- **Comments** you write on others' content;

- **Reactions and interactions** with community content;
- **Community connections** (follows, friends, or group memberships you initiate).

The visibility of this data depends on your privacy settings. Content you mark as public is viewable by other VitaNexus users. Content you mark as private remains visible only to you unless you choose to share it.

D. Usage and Analytics Data

To maintain and improve the Application, we automatically collect certain usage and technical data:

- **App session data** — when you open and close the app, session duration;
- **Feature interaction data** — which features you use and how frequently;
- **Crash reports** — automated diagnostic data generated when the app crashes;
- **Performance data** — app load times, error rates, and responsiveness metrics.

This data is used solely to operate, maintain, and improve the Application. It is anonymized after 12 months.

E. Device and Technical Data

We collect limited technical data about the device and environment used to access VitaNexus:

- **Device type and model;**
- **Operating system version** (iOS or Android);
- **Application version;**
- **IP address** (used for security and fraud prevention purposes);
- **Device identifiers** (such as advertising identifiers, where permitted and applicable).

F. Location Data

VitaNexus collects **approximate location data only**, and only with your explicit permission. We do not track precise GPS location without a clear, separate, affirmative consent request explaining the specific purpose. Approximate location may be used to provide region-relevant content or comply with applicable law. You may revoke location permissions at any time through your device settings.

G. Support Data

When you contact VitaNexus customer support, we collect the content of your communications — including messages, attachments, and contact details — solely to respond to your inquiry and to improve support quality. Support communications are retained for 24 months from the date of the interaction and are accessible only to authorized support personnel.

3. Data Classification

VitaNexus classifies data by sensitivity level to determine appropriate access controls, handling procedures, retention periods, and sharing permissions. The table below summarizes our classification framework.

Data Type	Sensitivity Level	Retention Period	Sharing Permissions
Account Data (name, email, username, password hash, profile photo)	Medium	Active period + 90 days post-account deletion	Shared only with service providers necessary for account operation (e.g., authentication, email delivery). Not sold. Not shared with advertisers.
Wellness and Lifestyle Data (mood, activity, goals, journals, sleep)	Medium-High	Active period + 90 days post-account deletion; then permanently deleted or fully anonymized	Never shared with third parties without explicit, informed user consent. Never used for advertising targeting. Never shared with health insurers, employers, or clinical providers.
Social and Storytelling Data (posts, stories, comments, interactions)	Low–Medium (visibility determined by user privacy settings)	Active period + 30 days post-deletion request	Shared within the VitaNexus community per user privacy settings. Aggregate, anonymized content trends may be used for product research.
Usage and Analytics Data (sessions, features, crashes, performance)	Low	24-month rolling window; anonymized after 12 months	Used internally for product improvement. Aggregate, anonymized analytics may be shared with development partners. Not linked to individual user identities after anonymization.
Device and Technical Data (device type, OS, app version, IP, identifiers)	Low	12-month rolling window	Used internally for security, fraud prevention, and technical support. IP addresses are not retained beyond 12 months except where legally required.
Location Data (approximate only)	Medium	Session-level; not persistently stored beyond current session	Not shared with third parties. Not used for precise tracking or profiling.

Data Type	Sensitivity Level	Retention Period	Sharing Permissions
		unless required for a specific opted-in feature	
Support Data (support communications)	Medium	24 months from date of interaction	Accessible only to authorized support personnel. Not shared externally except where legally required.

4. How We Protect Your Data

VitaNexus applies a layered, defense-in-depth security architecture. While no system can guarantee absolute security, our controls are designed to meet or exceed industry standards for consumer wellness applications. The following describes our key security measures across five domains.

A. Encryption

4.A.1 Data at Rest. All user data stored on VitaNexus infrastructure is encrypted using **AES-256** (Advanced Encryption Standard with 256-bit keys), the current industry standard for strong symmetric encryption. This applies to all databases, file storage systems, and backup media containing user data.

4.A.2 Data in Transit. All data transmitted between your device and VitaNexus servers is protected using **TLS 1.2 or TLS 1.3** (Transport Layer Security). Older, less secure protocol versions (SSL, TLS 1.0, TLS 1.1) are explicitly disabled across all VitaNexus endpoints.

4.A.3 Database-Level Encryption. Databases containing wellness and account data are encrypted at the database level in addition to disk-level encryption, providing multiple layers of protection against unauthorized access.

B. Access Controls

4.B.1 Role-Based Access Control (RBAC). Internal access to VitaNexus systems is governed by a formal role-based access control framework. Every employee and contractor is granted only the access necessary to perform their specific job function — no more.

4.B.2 Principle of Least Privilege. Access rights are provisioned at the minimum level required. Access is reviewed quarterly and revoked immediately upon role change or termination.

4.B.3 Multi-Factor Authentication (MFA). Multi-factor authentication is required for all internal systems and administrative interfaces. No internal system access is permitted on password alone.

4.B.4 Individual Wellness Data Access. No VitaNexus employee may access an individual user's wellness journal entries, mood data, or goal records except in two narrow circumstances: (1) with the user's explicit, documented consent in connection with a support request, or (2) when legally compelled by a valid court order or lawful government process.

C. Infrastructure Security

4.C.1 Cloud Infrastructure. VitaNexus is hosted on SOC 2 Type II compliant cloud infrastructure provided by **Microsoft Azure**. SOC 2 Type II compliance means our hosting provider has undergone independent third-party audits confirming its security, availability, and confidentiality controls over an extended audit period.

4.C.2 Network Perimeter Defenses. VitaNexus employs a Web Application Firewall (WAF) to filter malicious traffic, distributed denial-of-service (DDoS) protection to maintain service availability, and network-level intrusion detection systems.

4.C.3 Continuous Monitoring. Security events are logged and monitored continuously. Automated alerting is in place for anomalous access patterns, failed authentication attempts, and other indicators of compromise.

D. Application Security

4.D.1 Secure Software Development Lifecycle (SSDLC). Security is integrated into every phase of VitaNexus software development — from design and threat modeling through coding, testing, and deployment. We do not release code that has not completed a security review gate.

4.D.2 Code Review and Security Testing. Every release undergoes peer code review and automated security testing, including static analysis (SAST) and dependency vulnerability scanning, before it reaches production.

4.D.3 API Authentication. All VitaNexus APIs are protected by modern authentication standards, including **OAuth 2.0** for delegated authorization and **JWT (JSON Web Tokens)** for session management. Tokens are short-lived and rotated regularly.

4.D.4 Input Validation and Output Encoding. VitaNexus implements strict input validation and output encoding across all user-facing interfaces to prevent injection attacks, cross-site scripting (XSS), and related vulnerabilities.

E. Third-Party Security

4.E.1 Vendor Security Standards. All third-party vendors and service providers who handle VitaNexus user data are contractually required to meet VitaNexus security standards, which align with SOC 2 principles and applicable privacy regulations.

4.E.2 Data Processing Agreements (DPAs). VitaNexus executes Data Processing Agreements with all data processors, defining permitted uses of data, security obligations, breach notification requirements, and data return or destruction obligations upon contract termination.

4.E.3 Vendor Assessments. Prospective vendors who will access or process user data undergo a security assessment before onboarding. Existing vendors are subject to periodic reassessment. Vendors that do not meet our standards are not onboarded or are terminated.

5. Data Storage and Retention

5.1 Storage Location

VitaNexus user data is stored on servers located in the **United States** on Microsoft Azure infrastructure. VitaNexus offers its services only to users in the United States and maintains all primary data storage domestically.

5.2 Retention by Data Type

Retention periods by data category are set out in the Data Classification table in Section 3 of this Policy. In summary:

- **Account and Wellness Data:** Retained for the duration of your active account, plus 90 days following account deletion to accommodate recovery requests and fulfill legal obligations.
- **Social/Storytelling Data:** Retained for the duration of your active account, plus 30 days following deletion.
- **Usage/Analytics Data:** Retained on a 24-month rolling basis; anonymized at the 12-month mark.
- **Device/Technical Data:** Retained on a 12-month rolling basis.
- **Support Communications:** Retained for 24 months from the date of interaction.

5.3 Account Deletion and Data Removal

When you delete your VitaNexus account, we will permanently delete your personal data — including all wellness entries, account information, and social content — within **90 days** of the confirmed deletion request. You will receive a confirmation when deletion is complete. After the 90-day period, your data will not be recoverable.

5.4 Anonymization and Aggregation

Where data is retained after deletion for legitimate purposes such as analytics, product improvement, or legal compliance, it will be **fully anonymized and aggregated** such that it cannot be used to identify any individual user. Anonymized data retained for these purposes is not subject to deletion requests, as it no longer constitutes personal data.

5.5 Backup Retention

VitaNexus maintains encrypted system backups on a **30-day rolling basis**. Backups are subject to the same encryption standards (AES-256) as primary data storage. Backups are not used to circumvent deletion requests — upon expiration of the 90-day deletion window, backups containing deleted user data are overwritten or purged.

6. Data Sharing and Disclosure

6.1 With Whom We Share Data

VitaNexus shares user data only in the following limited circumstances:

- **Service Providers:** We share data with third-party service providers who perform functions on our behalf — such as cloud hosting, email delivery, analytics processing, and customer support tooling. These providers are contractually bound by our Data Processing Agreements and may not use data for any purpose other than providing the contracted service.
- **Legal Authorities:** We may disclose data when required by applicable law, regulation, court order, or lawful government request. Where legally permitted, we will notify affected users before making such a disclosure.
- **Business Transfers:** In the event of a merger, acquisition, asset sale, or corporate reorganization involving VitaNexus, user data may be transferred to the acquiring entity. We will provide users with advance notice of any such transfer via in-app notification and email, and users will have the opportunity to delete their accounts before the transfer occurs.

6.2 What We Do Not Do

Data Sharing Prohibitions

VitaNexus commits, without exception, to the following restrictions on data sharing:

• We do **NOT** sell your personal data to any third party.

• We do **NOT** share wellness data with health insurers, life insurers, employers, or third-party marketers without your explicit, informed, and revocable consent.

• We do **NOT** share user data with healthcare providers or clinical systems — VitaNexus is not a clinical platform and has no data exchange relationship with any clinical entity.

• We do **NOT** use wellness data to build advertising profiles or to target advertisements to users.

6.3 Aggregate and Anonymized Analytics

VitaNexus may share aggregate, fully anonymized analytics data with development partners, academic researchers, or the public for purposes of product research, wellness trend analysis, or application improvement. Anonymized data cannot be used to identify individual users and does not constitute personal data under applicable law.

7. User Data Rights and Controls

VitaNexus believes that your data belongs to you. We provide the following rights to all users, and extend additional jurisdiction-specific rights where required by law.

7.1 Universal User Rights

Right	Description	How to Exercise
Access	Request a complete copy of the personal data VitaNexus holds about you.	Submit a request to **privacy@vitanexus.ai** or via the in-app "My Data" settings.
Correction	Update or correct inaccurate or incomplete information in your account.	Update directly in Account Settings, or contact **privacy@vitanexus.ai**.
Deletion	Request permanent deletion of your account and all associated personal data.	Use the "Delete Account" option in Account Settings, or email **privacy@vitanexus.ai**.
Portability	Download a copy of your wellness data in a structured, machine-readable format (JSON or CSV).	Use the "Export My Data" option in Account Settings.
Opt-Out	Opt out of optional analytics tracking, marketing communications, and optional data collection features at any time.	Manage preferences in Privacy Settings within the App, or contact **privacy@vitanexus.ai**.

7.2 California Residents (CCPA)

If you are a California resident, you have the following additional rights under the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA):

- The right to know the categories and specific pieces of personal information collected about you;
- The right to know the categories of third parties with whom your information is shared;
- The right to opt out of the sale or sharing of your personal information (VitaNexus does not sell personal information);
- The right to limit the use and disclosure of sensitive personal information;
- The right to non-discrimination for exercising your privacy rights.

To submit a California-specific request, email **privacy@vitanexus.ai** with "CCPA Request" in the subject line.

7.3 Other State Privacy Rights

Residents of certain other US states — including Virginia (VCDPA), Colorado (CPA), Connecticut (CTDPA), Utah (UCPA), Texas (TDPSA), and Oregon (OCPA) — may have additional rights, such as the rights to access, correct, delete, and obtain a portable copy of their personal data, and to opt out of certain processing. To exercise any such rights, contact **privacy@vitanexus.ai**. We will honor verified requests as required by the applicable state law.

7.4 Response Time

VitaNexus will respond to all data rights requests within **30 days** of receipt. In cases of complexity or high volume, we may extend this period by an additional 30 days, with prior notice to you.

8. Children's Data

8.1 Age Restriction

VitaNexus is **not directed to children under the age of 13**. We do not knowingly collect personal data from any individual under the age of 13. Users must be at least 13 years of age to create a VitaNexus account. Users between the ages of 13 and 17 may be subject to additional restrictions depending on their jurisdiction.

8.2 COPPA Compliance

VitaNexus complies with the Children's Online Privacy Protection Act (COPPA). We do not knowingly collect, store, or process personal information from children under 13. Our registration process includes age verification mechanisms designed to screen out underage users.

8.3 Discovery and Removal

If VitaNexus discovers that a user account belongs to a child under 13, we will promptly:

- Suspend the account;
- Delete all associated personal data; and
- Notify a parent or guardian if contact information is available.

8.4 Parental Removal Request

If you are a parent or legal guardian who believes your child under the age of 13 has created a VitaNexus account without your consent, please contact us immediately at **privacy@vitanexus.ai** with "COPPA — Parental Removal Request" in the subject line. We will verify the request and delete the account and associated data within 10 business days of verification.

9. Incident Response and Breach Notification

9.1 Detection and Initial Response

VitaNexus maintains a formal Security Incident Response Plan (SIRP) that governs how we detect, triage, and respond to security events. Our continuous monitoring systems — including intrusion detection, anomaly alerts, and vendor security feeds — are designed to surface potential security incidents rapidly.

9.2 Internal Escalation and Containment

Upon detecting a potential security incident, our process includes:

1. **Initial Triage:** The security team classifies the event by severity and scope.
2. **Escalation:** Incidents meeting defined severity thresholds are escalated immediately to the Security Lead, CTO, and legal counsel.
3. **Containment:** Affected systems are isolated or access is revoked to prevent further exposure.
4. **Forensic Investigation:** A root cause analysis is conducted to determine the nature, scope, and origin of the incident.
5. **Eradication:** The underlying vulnerability or threat is addressed and remediated.
6. **Recovery:** Affected systems are restored to normal operation with enhanced monitoring in place.

9.3 User Notification

In the event of a confirmed data breach that affects your personal data, VitaNexus will notify you **within 72 hours** of confirmation, where legally required. Notification will be provided via email to the address associated with your account and, where feasible, via in-app alert. The notification will describe:

- The nature of the breach and what data was affected;
- The likely consequences of the breach;
- The steps VitaNexus has taken or will take to address it; and
- Actions you can take to protect yourself.

9.4 Regulatory Cooperation

VitaNexus will cooperate fully with applicable regulatory authorities in the event of a security incident, including the FTC and state attorneys general. We will provide required notifications to regulators within the timeframes mandated by law.

9.5 Post-Incident Review

Following every significant security incident, VitaNexus conducts a formal post-incident review to identify root causes, assess the effectiveness of our response, and implement improvements to prevent recurrence. Findings from post-incident reviews are incorporated into updated security controls and training programs.

9.6 Security Disclosure Contact

If you discover a potential security vulnerability in the VitaNexus Application or infrastructure, we encourage responsible disclosure. Please report your findings to **security@vitanexus.ai**. We are committed to acknowledging receipt within 2 business days and to working collaboratively with good-faith security researchers to resolve verified issues.

10. Compliance and Certifications

VitaNexus aligns its data practices with the following regulatory frameworks and platform standards. Compliance with these frameworks reflects our commitment to user trust, legal integrity, and responsible data stewardship.

Framework / Standard	Applicability and VitaNexus Position
CCPA / CPRA (California Consumer Privacy Act / California Privacy Rights Act)	VitaNexus complies with CCPA/CPRA requirements for California residents, including rights of access, deletion, correction, portability, and opt-out from sale. VitaNexus does not sell personal data.
Other State Privacy Laws (VA, CO, CT, UT, TX, OR)	VitaNexus honors applicable rights under comprehensive state privacy laws including the VCDPA, CPA, CTDPA, UCPA, TDPSA, and OCPA for residents of those states.
COPPA (Children's Online Privacy Protection Act)	VitaNexus does not collect personal information from children under 13. COPPA compliance procedures are described in Section 8 of this Policy.
FTC Act — Section 5	VitaNexus commits to avoiding unfair or deceptive data practices as governed by Section 5 of the Federal Trade Commission Act. Our data representations in this Policy and in-app disclosures are accurate and substantiated.
Apple App Store — Data Safety	VitaNexus complies with Apple's App Privacy requirements, including accurate App Store privacy nutrition labels disclosing data types collected, data linked to identity, and data used for tracking.
Google Play — Data Safety Section	VitaNexus complies with Google Play's Data Safety requirements, including accurate disclosure of data collection, sharing, and security practices in the Data Safety section of our Play Store listing.
SOC 2 Type II (via infrastructure provider)	VitaNexus is hosted on SOC 2 Type II compliant Microsoft Azure cloud infrastructure, providing independent third-party assurance of security, availability, and confidentiality controls.

HIPAA and FDA Non-Applicability — Explicit Statement

VitaNexus is NOT a HIPAA-covered entity and does not handle Protected Health Information (PHI). HIPAA does not govern VitaNexus's data practices. **VitaNexus is NOT regulated by the FDA as a medical device** and has not been cleared or approved by the FDA for any clinical or diagnostic purpose. These are not gaps — they are accurate reflections of what VitaNexus is: a consumer wellness and social storytelling application.

11. Wellness Data — Special Handling

VitaNexus treats wellness and lifestyle data — including mood entries, activity logs, wellness journal entries, goal records, and sleep inputs — with a **heightened level of sensitivity and care** that exceeds our general data protection standards. The following rules apply specifically and exclusively to wellness data.

11.1 Elevated Storage Standards

All wellness data is stored with database-level AES-256 encryption. Access to wellness data at the record level is restricted to a narrow class of authorized personnel, none of whom may access individual entries except in the limited circumstances described in Section 4.B.4.

11.2 No Advertising Use

Wellness data is **never** used to build advertising profiles, to target or personalize advertisements, or to inform any advertising-related decision. This prohibition applies absolutely — it cannot be waived by platform-wide settings, and wellness data will never be shared with advertising technology providers.

11.3 No Third-Party Sharing Without Explicit Consent

Wellness data is **never** shared with any third party — including research institutions, analytics providers, wellness partners, or any other entity — without your explicit, informed, specific, and revocable consent. General consent to our Terms and Conditions does not constitute consent to share individual wellness data.

11.4 No Clinical Conclusions

> **Critical Limitation — Wellness Data Cannot Support Clinical Conclusions**
>
> Wellness data entered into VitaNexus — regardless of how much data you have entered or over what period — **cannot be used to draw clinical, diagnostic, or medical conclusions**. VitaNexus is not a clinical measurement tool. Its inputs are self-reported. Its features are designed for personal reflection and self-awareness, not medical analysis. Do not use patterns, trends, or summaries visible in VitaNexus to make medical decisions. Always consult a licensed healthcare professional before taking any health-related action.

11.5 User Control

You retain full control over your wellness data at all times. You may:

- Delete individual wellness entries at any time from within the App;
- Export all of your wellness data in machine-readable format;
- Request complete deletion of all wellness data upon account closure; and

- Opt out of any optional wellness data features at any time.

12. Third-Party Integrations

12.1 Optional Integrations

VitaNexus may offer optional integrations with third-party wellness and fitness platforms, such as **Apple Health** (iOS) and **Google Fit** (Android). These integrations are entirely optional and are activated only by explicit user choice.

12.2 Data Flows

When you enable a third-party integration, you will be presented with a clear description of:

- What data will flow **from** the third-party platform **into** VitaNexus;
- What data, if any, will flow **from** VitaNexus **to** the third-party platform;
- The purpose for which that data will be used within VitaNexus; and
- How to disconnect the integration.

You must provide affirmative consent to each integration before any data exchange begins. Consent is recorded and auditable.

12.3 User Control Over Integrations

You may disconnect any third-party integration at any time from within the App's Settings menu. Upon disconnection, VitaNexus will cease receiving new data from the third-party platform. Data previously received through the integration will be subject to our standard retention and deletion policies.

12.4 Third-Party Data Practices

VitaNexus is **not responsible** for the data practices, privacy policies, or security measures of third-party platforms. When you use an integration, your data on the third-party platform is governed solely by that platform's terms and privacy policy. We encourage you to review those documents carefully before enabling any integration.

13. Contact and Responsible Disclosure

VitaNexus maintains dedicated contact channels for data-related inquiries, security disclosures, and user rights requests. We are committed to responding promptly and substantively to all good-faith communications.

Contact VitaNexus

Topic	Email
Privacy questions	privacy@vitanexus.ai
Security issues / vulnerability reports	security@vitanexus.ai
Legal / Terms questions	legal@vitanexus.ai
General support	support@vitanexus.ai
Founder / executive contact	founders@vitanexus.ai

Website: vitanexus.ai

VitaNexus does not tolerate harassment, threats, or public disclosure of unverified vulnerabilities. We ask security researchers to provide us with a reasonable opportunity to investigate and remediate before any public disclosure. We will not pursue legal action against good-faith security researchers who follow responsible disclosure practices.

14. Changes to This Policy

14.1 How We Notify You

VitaNexus may update this Data and Security Policy from time to time to reflect changes in our data practices, applicable law, or the features of the Application. When we make **material changes** to this Policy, we will notify you by:

- **In-app notification:** A clear notice will appear within the Application when you next open it, summarizing the changes and linking to the updated Policy;
- **Email:** Where we have your email address, we will send a notification to your registered email address summarizing the material changes.

14.2 Effective Date

The effective date at the top of this Policy reflects when the current version took effect. Prior versions of this Policy will be archived and available upon request by emailing **privacy@vitanexus.ai**.

14.3 Continued Use

Your continued use of VitaNexus following the effective date of a revised Policy constitutes your acceptance of the changes. If you do not agree to the revised Policy, you may delete your account before the effective date in accordance with the procedures described in Section 7.

> **Note on Non-Material Changes**
>
> Minor updates — such as corrections of typographical errors or clarifications that do not affect your rights — may be made without advance notice. The “Last Updated” date at the top of this Policy will always reflect the most recent revision, including minor updates.

IMPORTANT NOTICE — NOT A MEDICAL SERVICE

VitaNexus is a wellness and social storytelling application only. It is not a medical device, is not a HIPAA-covered entity, and does not collect, process, or store clinical health data or Protected Health Information (PHI) of any kind. VitaNexus has not been cleared or approved by the U.S. Food and Drug Administration (FDA) for any clinical, diagnostic, or treatment purpose.

Wellness data recorded in VitaNexus is not a substitute for professional medical advice, clinical diagnosis, or treatment. Patterns, trends, or summaries visible within the Application are for personal awareness only and carry no clinical validity. **Always consult a qualified and licensed healthcare professional for any health concerns before taking medically relevant action.**

VitaNexus is not for emergency use. If you are experiencing a medical emergency, call 911 or your local emergency services immediately.

VitaNexus Data and Security Policy | Version 1.0 | Effective: June 11, 2026 | Last Updated: June 11, 2026
 | privacy@vitanexus.ai | security@vitanexus.ai