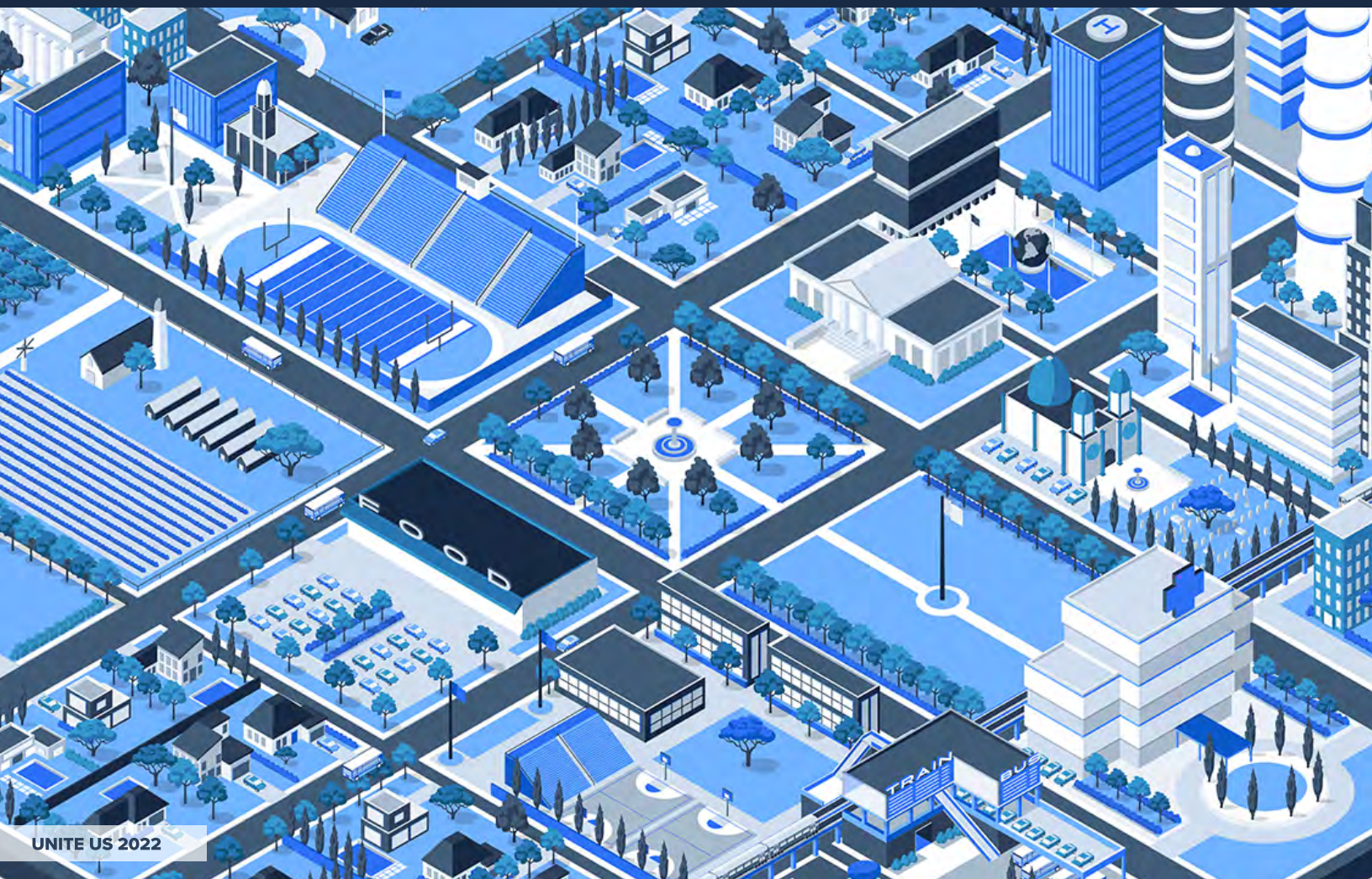
UNITE US

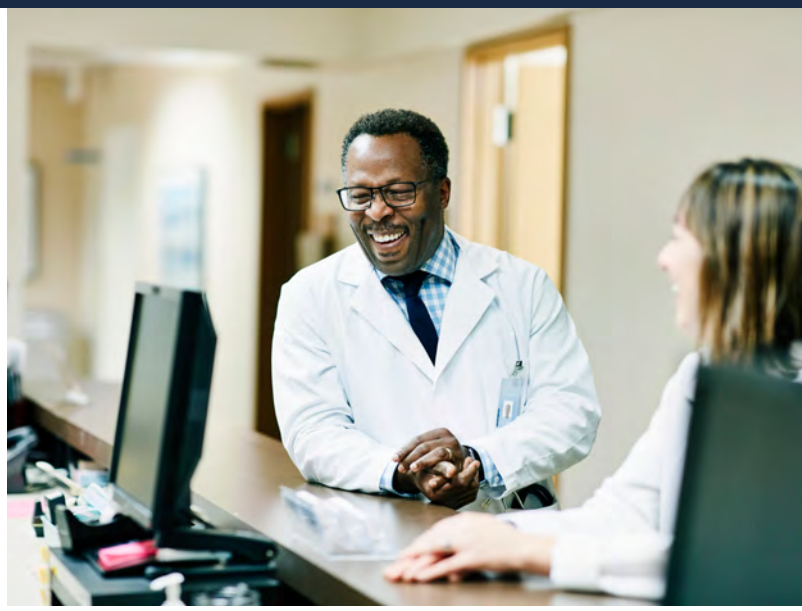
Security Overview

Last Updated May 2023



Contents

01 Overview



Security Program

Unite Us offers a Cloud-based, commercially available, software-as-a-service solution that is utilized and trusted by thousands of organizations across the country. Since its inception in 2013, Unite Us has prioritized implementing the controls necessary to maintain the confidentiality and integrity of all data stored in our platform, including protected health information (PHI) and personally identifiable information (PII). Unite Us takes pride in our culture of compliance, which combines cross-team collaboration and training with industry-leading security certifications to ensure that our systems are trusted and secure. We have implemented extensive security controls in line with the HITRUST Common Security Framework, the NIST Cybersecurity Framework, and SOC 2 Type II compliance to ensure our architecture and infrastructure is protected from end to end. This document provides an overview of the compliance and security processes and standards implemented across our organization.

Regulatory Compliance

Unite Us is considered a Business Associate to Covered Entities utilizing our platform, as defined under the Health Insurance Portability and Accountability Act (HIPAA). As a Business Associate, Unite Us has implemented regular risk assessments; technical, physical, and administrative safeguards; audit logging and monitoring; access controls aligned with the minimum necessary standard; and breach-notification policies. Unite Us routinely signs Business Associate Agreements (BAAs) with Covered Entities where applicable.

In addition to Unite Us being fully HIPAA compliant, Unite Us also aligns with the strictest federal and state privacy regulations, including 42 CFR Part 2, FERPA, VAWA, and the CCPA. Unite Us' enhanced access controls allow users to exchange regulated information in a way that complies with applicable law.

02
Security Certifications

The HITRUST Common Security Framework is a comprehensive and rigorous security framework that is considered the industry gold standard in certifying privacy and security compliance, especially within the healthcare industry. The Unite Us Platform is HITRUST certified with a scope to HIPAA and CCPA. You can view our certification letter in the **Supporting Materials** section of this document.

The **NIST security framework** is an overarching, industry-agnostic framework that assesses whether organizations have implemented robust risk-management principles and best practices to help improve the security and resilience of critical infrastructure. Unite Us can provide a copy of our most recent NIST Certification report if your organization has signed an NDA or another confidentiality agreement with Unite Us.

SOC 2 Type II certification is based on a cybersecurity-compliance security framework covering principles such as security and privacy. SOC 2 Type II audits assess how well an organization protects consumer data and information through its business operations. Comprehensive SOC 2 Type II reports are issued by independent auditors on an annual basis. Unite Us can provide a copy of our most recent SOC 2 Type II report if your organization has signed an NDA or another confidentiality agreement with Unite Us.

03
Cloud Security

Amazon Web Services
Unite Us is a Cloud-based solution fully hosted by Amazon Web Services (AWS). AWS holds a range of certifications, including HITRUST, SOC 1, 2, and 3, ISO 27001, and FedRAMP. Through AWS, the best security professionals in the industry protect our data infrastructure. You can find more information about AWS' industry-leading security controls here.

Encryption Standards
Unite Us encrypts all data at rest and in transit, pursuant to policy and technical control. At rest, data is stored on encrypted volumes using AWS Key Management Services (AWS KMS). Each volume is encrypted with a unique AES 256-bit key. In transit, data is transmitted using TLS 1.2 certificates with 256-bit encryption.

Key Management
All keys are protected by AWS' key management infrastructure, which implements strong logical and physical security controls to prevent unauthorized access. AWS' overall key management infrastructure uses Federal Information Processing Standards (FIPS) 140-2 approved cryptographic algorithms and is consistent with NIST recommendations.

Endpoint Monitoring
All Unite Us user endpoints are continuously monitored by a mobile device management (MDM) solution. The MDM solution provides real-time management and alerting capabilities.

DDoS Attack Prevention
Unite Us deploys internet-facing boundary protections to block traffic that would allow for degradation or denial of service from external sources.

Firewalls
As part of Unite Us' multilayered approach to security and prevention, we utilize a Cloud-based firewall that performs malware scanning, vulnerability scanning, URL filtering to prevent connections to malicious and high-risk sites, and content scanning to prevent the exfiltration of sensitive information from our systems. In keeping with best practices, we have enabled audit logging for all activity, which is stored in a secure, remote location for monitoring and analysis.

Business Continuity and Disaster Recovery
Unite Us maintains a robust and regularly updated Business Continuity and Disaster Recovery (BCDR) plan and can provide a copy of this documentation with a signed NDA. The BCDR plan is reviewed and tested at least annually by an independent, third-party auditor, and includes the following Recovery Time Objective (RTO) and Recovery Point Objective (RPO) standards: The RTO of the product is within 0–12 hours, where mission critical services will be restored first, followed by secondary services. RPO is one (1) hour.

The Unite Us Platform architecture leverages horizontal scaling across its infrastructure. Data stores are clustered with automated failover/reorganization in the event of individual instance failures.

Availability
The Unite Us Platform maintains a standard uptime service level of 99.9% availability, with historical uptime exceeding this level.

Data Residency and Redundancy
All data is maintained within domestic data centers. No data is accessed or transmitted outside of the United States. All data is housed in a primary data center as well as a backup data center, which are geographically dispersed to ensure redundancy of information.

04
Product Security

Network Architecture
Unite Us constructed its network architecture to provide multiple layers of security to protect information and data contained within the platform. Unite Us can provide a copy of its network architecture diagram with a signed NDA.

Penetration Testing
Unite Us engages third-party auditors to conduct penetration testing on an annual basis at minimum, or more frequently if needed, at Unite Us' discretion. Results of the most recent penetration test are available with a signed NDA.

Vulnerability Management
Unite Us conducts continuous vulnerability monitoring of its environment, which runs 24x7x365, with real-time alerts in the event an anomaly is detected. In addition, file-integrity monitoring detects changes to system binaries, libraries, and configuration files, while host-activity monitoring detects package installation and any potentially malicious user activity. In addition, package-vulnerability scanning warns of potential exploits to software and code.

Secure Development Lifecycle
Unite Us follows a Secure Development Lifecycle (SDLC) process for all of its development and product creation. The Unite Us SDLC policy embeds testing throughout the software development lifecycle to ensure quality control measures are followed. Methods for testing can include unit testing, integration testing, performance testing, and security testing, with development in line with OWASP security standards. All relevant team members complete OWASP secure code training upon hire, and at least annually thereafter.

Data Loss Prevention
Unite Us has deployed extensive data loss prevention (DLP) solutions. The DLP structure is enforced through a combination of policy, technical controls, and third-party tools that are all used in conjunction to identify, isolate, and block the unapproved or unintended exfiltration of sensitive data from within Unite Us systems. The DLP solutions apply to all workforce members and devices.

05
IT Security

Endpoint Protection

Unite Us issues endpoint devices to all team members. The devices are equipped with a mobile device management (MDM) solution, and both the MDM solution and the devices themselves are centrally managed by the Unite Us IT department. Endpoints are equipped with antivirus software, malware detection capabilities, and full disk encryption. Endpoints are assigned to individual users and require unique credentials, including biometrics, to access the device.

User Authentication

Unite Us ensures user authentication via unique login and passwords, but also provides two-factor authentication options to all end users free of charge. In addition, Unite Us supports SAML 2.0-based authentication integrations. Internally, all Unite Us teams are authenticated via enterprise-wide, multi-factor identity verification protocols.

Access Controls

Every Unite Us user is configured with individual viewing permissions based on their role and responsibilities. These permissions align with the HIPAA minimum necessary standard, and the NIST principle of least privilege. Internally, Unite Us enforces strict, role-based access to information, and all access credentials are regularly reviewed. Unite Us supports audit logging and monitoring, and all user activity within the platform is captured in audit logs.

Physical and Environmental Security

Robust physical and environmental security controls are in place within Unite Us office spaces. Measures include, but are not limited to, key card access, cameras, protected wireless access points, visitor access protocols, and fire safety measures. No data is housed within Unite Us physical office spaces. Physical and environmental security of data centers is managed and controlled by AWS.

06 Consent and Privacy

Unite Us is built upon a foundation of privacy and security. At Unite Us, no referral can be shared without the individual's documented consent. The consent form helps an individual understand how their information may be shared in order to connect them to services. Consent is required and documented for every referral made through the Unite Us Platform for the client. Individuals can revoke their consent at any time for any reason, and the methods for revoking consent are listed directly within the consent form. Additionally, if an organization is also required to capture a subject-matter or organizational-specific consent as required by law or policy, such as a 42 CFR Part 2–specific consent, then they should continue to do so. Those organizations can also upload those subject-matter-specific consent documents directly within the client record in Unite Us.

The Unite Us consent links to our publicly available privacy policy and is written with health equity, literacy, and accessibility concerns in mind. The consent is accessible in more than 50 languages and is available in multiple formats to support accessibility.

Our publicly available privacy policy outlines the ways in which information may be shared via our platform. A full version of our privacy policy is available **here**.

07 Administration and Operations

Workforce Screening

Unite Us conducts screenings and background checks on all workforce members upon hire. These background checks include nationwide criminal database screenings; background verifications; Social Security Number verifications; SAM, OIG, and OFAC exclusions; FBI watchlist checks; and healthcare sanctions screenings upon hire and monthly thereafter.

Training

All Unite Us workforce members undergo extensive compliance training upon hire, annually thereafter, and more frequently in the event of a major change. Training courses include, but are not limited to, HIPAA Compliance, Information Security Awareness, Sexual Harassment Prevention, and Secure Code Training.

08
Supporting Materials

Unite Us provides the following materials to customers without an NDA:

- HITRUST Certification Letter
- Consent and Privacy Policy

Unite Us can provide the following documentation upon the execution of an NDA:

- SOC 2 Type II Report
- Business Continuity and Disaster Recovery Plan
- Annual Penetration Testing Report
- Annual Risk Assessment Report
- Annual Disaster Drill Report
- Policies and Procedures
- Network Architecture Diagram

Learn more at
www.UniteUs.com

UNITE US