Trustworthy.

Trustworthy Security

Trustworthy is built with world-class security technologies, employs strict policies to protect member information, and is leading the industry by adopting privacy-preserving technologies like end-to-end encryption for data.

Here's a breakdown of the different security elements Trustworthy employs to help keep member data safe, secure and private.

Multi-factor authentication

To create an account with Trustworthy, you need an email address and password. Each member's email address is unique, and our password recipe requires a minimum of 8 characters, including numbers, symbols, and upper- and lowercase letters.

Trustworthy also requires two-factor authentication as a default — not an option — to verify a member's identity. It's an extra layer of security for Trustworthy accounts designed to ensure that members are the only people who can access their account, even if someone else knows their password.

With two-factor authentication, only members can access their account on a trusted device or the web. When you want to sign in to a new device for the first time, you'll need to provide two pieces of information: your password and a one-time, random, six-digit verification code automatically sent to your phone. By entering the code, you verify that you trust the new device.

Multiple layers of security — a password and two-factor authentication — dramatically improve the security of your Family Operating System® and aid in protecting you from phishing attacks.

Physical security keys

Security hardware (tokens or keys) allows users to add a second authentication factor to online services.

One common security key is a YubiKey. It looks similar to a USB thumb drive and is physically attached to the device you're using to authenticate. You must be physically present to authenticate a YubiKey. Yubikeys is one of the best ways to avoid phishing and account takeovers.

Trustworthy is the only family information platform that supports security hardware. Security keys are optional. Support for security hardware is available in the Gold plan. Email support@trustworthy.com to learn more.

Biometric authentication

Trustworthy employs biometric (facial or fingerprint) authentication on our mobile app and on desktop. This is an additional layer of authentication with added convenience to members quickly access their information.

Data encryption

Trustworthy data is encrypted in transit and at rest to provide the highest level of data security. This means that member data is protected with a key derived from information unique to your account, combined with your device passcode, which only you know. No one else can access or read this data.

All the information you enter into Trustworthy is transmitted and stored using the AES 256-bit encryption key.

Even if someone were to breach Trustworthy and get your data, they would need access to Trustworthy encryption keys to decrypt it and read it. Without the 256-bit encryption keys, the information would be hashed and unreadable.

A hacker would require 2 to the power of 256 different combinations to break a 256-bit encrypted message, which is extremely difficult to be broken by even the fastest computers. For reference, the U.S. government requires that all sensitive and important data be encrypted using 192- or 256-bit encryption methods.

On-screen redaction

Trustworthy redacts sensitive information (such as a driver's license number) in the user interface to ensure that prying eyes cannot see the information on your device screen.
To protect your information in public places, we also recommend using a privacy screen for your devices.

Tokenization and aliasing

Trustworthy uses a next-generation security technique called tokenization (aliasing) to protect member information. Tokenization removes sensitive data from the Trustworthy application database and replaces it with a corresponding token, keeping the sensitive information protected and separate from the member's account.

SOC-2 Compliance

Trustworthy is in the process of securing SOC-2 compliance. SOC-2 compliance is.... We expect to be in full compliance by fall 2021, and are already more compliant than many providers.

Artificial intelligence

Trust, privacy and transparency have always been at the core of Trustworthy, and our work with artificial intelligence (AI) is no different.

Trustworthy does not use data from customers to train AI models.

Trustworthy uses AI in a way that is "memoryless" - the model does not change or update when we interact with it, and your information is not learned by the model. While there are existing AI-powered services that do update or learn from your information, this is not something that is innate to using AI models. The processes of "reasoning" (i.e. asking the model questions about a given document) and "learning" (i.e. instructing the model to remember details of a given document) are entirely separate. We use AI models exclusively for their reasoning capabilities, and do not update based on any data provided by our users. It is not possible for "learning" to occur unintentionally.

In addition, when working with third-party models running on the Trustworthy private cloud, Trustworthy and its partners agree on robust protections to safeguard the data privacy and security of our customers and users.

Partners

Trustworthy works with various security providers to enhance our security stack. We only work with providers who achieve the highest levels of security and privacy.

Member data may be stored using third-party partners' secure cloud infrastructure to provide secure software services to members. Data stored in secure cloud infrastructure is not used for training or the benefit of third-party partner services.

Business model

Trustworthy revenue comes from subscribers — not advertisers. We believe that when you don't pay for the product, you are the product. Our business is underpinned by three core tenets - Private, Protected, & Yours.

Private: We'll never share or sell your family information.

Protected: Your family information is protected at all times by 256-bit encryption.

Yours: You are the arbiter of your data and can elect to remove it from our service at any time.

Trustworthy Employee Security

Every Trustworthy employee undergoes rigorous background and security checks before hiring and twice-annual security and privacy training to ensure they understand our commitment to keeping member information safe.

Employee company applications and devices are centrally managed by a third party, which allows our security team to remove access to business applications at will and remotely freeze or wipe devices as needed.

Security is built into everything we do. This isn't a platitude. It's a foundational part of our team culture. As we build Trustworthy, customer data is hidden at every step in the process so that customer information is never compromised.

Enterprise-grade compliance

General Data Protection Regulation (GDPR)

Trustworthy has worked to enhance our products, processes, and procedures to ensure our practices are GDPR-compliant.

GDPR is widely considered the world's strongest set of data protection rules, which enhance how people can access information about them and limit what organizations can do with personal data. While GDPR is not a requirement in the United States, Trustworthy meets all GDPR data privacy controls and standards to support its global members.

California Consumer Privacy Act (CCPA)

Trustworthy is a service provider to customers under the California Consumer Privacy Act (CCPA), and we fully support our customers' by compliance with the CCPA guidelines.

The California Consumer Privacy Act of 2018 (CCPA) gives consumers more control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law. This landmark law secures new privacy rights for California consumers, including:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale or sharing of their personal information and
- The right to non-discrimination for exercising their CCPA rights.

Enterprise-grade compliance

SOC-2 Type 2 Certification

Trustworthy is fully SOC2 Type 2 certified in accordance with the American Institute of CPAs (AICPA) SOC standard.

Compliance with SOC 2 requirements indicates that an organization maintains the highest level of information security. Strict compliance requirements (tested through independent audits) help ensure sensitive information is handled responsibly. Unlike SOC 2, Type 1, which assesses the design of controls at a specific point in time, Type 2 goes further by examining the operating effectiveness of those controls over a minimum of six months. This extended evaluation period is valuable because it allows organizations to demonstrate the consistency and durability of their control environment. Trustworthy is subject to annual (or more frequent) 3rd-party penetration testing.

SOC-3 Certification

Trustworthy is fully SOC3 certified in accordance with the American Institute of CPAs (AICPA) SOC standard.

SOC 3 reports are valuable for service organizations as they demonstrate their commitment to maintaining a high level of security and reliability for their clients. SOC 3 helps foster trust, enhance business relationships, and ensure that sensitive data is adequately protected, making it a vital component of today's information security landscape.

To request a copy of the Trustworthy SOC3 report, please email security@trustworthy.com.

HIPAA Compliance

Trustworthy is fully compliant with the standards set forth by the U.S. Department of Health and Human Services (HHS) in The Health Insurance Portability and Accountability Act (HIPAA) to ensure that any member's medical information is protected.

Visit trustworthy.com/security for more information