We are serious about security.

everplans®

Overview

Everplans takes your security extremely seriously. It wouldn't make sense to get into a business that deals with customers' extremely personal and sensitive information if security wasn't the highest of priorities. Our commitment, combined with a very fantastic and experienced engineering team, has resulted in a security environment that we feel very proud and confident in, and our goal is to inspire you to feel the same way. Below is a walkthrough of Everplans' approach to a number of different security-related topics.

Background

Everplans has been purpose-built from day one to be highly secure, using best of breed tools, software development methodologies and operational practices. This matters. Many of the high profile breaches at other companies over the past few years have occurred within large, old organizations that have been in the unenviable (and frankly untenable) position of trying to retro-fit, cobble together and secure multiple legacy systems that are ill-equipped to handle modern technology security needs.

Privacy

Everplans has put a great deal of thought and effort into creating a comprehensive Privacy Policy that can actually be read and understood by the average human being. Our Privacy Policy details exactly how different types of information are treated so all of our users can make educated decisions about what they feel comfortable including in their Everplans. The latest version can be found at: https://www.everplans.com/privacy-policy

HIPAA Compliance

In addition, Everplans has recently become compliant under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which means we manage the privacy and security of your information in accordance with the extremely formal and rigorous requirements of HIPAA, a compliance framework designed to protect sensitive personal and health information. We also execute Business Associate Agreements with any external parties through which your information is transmitted, holding them liable for protecting the privacy and security of your information to the same extent as us.

Our Security Framework

Everplans approaches security using the following framework:

- Securing your data at rest
- Securing your data in transit
- Operational procedures to keep the site secure
- Strict limitations around administrative access to your information
- Two factor authentication for end users

Securing Your Data at Rest

Within our systems, all your data is stored using AES-256 encryption with a uniquely derived key for each user as recommended by NIST Special Publication 800-132. We encrypt every single personally identifiable field in the database, including your name and email address. For searching and indexing, we hash a small number of fields using HMAC. We apply the same encryption technique to all files you upload.

What this means: *Your information is super-scrambled in the database which means employees can't see it and even if there were somehow a breach and someone got their hands on the data, they wouldn't be able to unscramble it to see what it says.*

Securing Your Data in Transit

All communications between you and Everplans are encrypted via SSL using 2048-bit certificates and we require SSL on all communications. We support perfect forward secrecy so that even if someone eavesdrops on your communication, they will still not be able to decrypt the data in the event that our key is compromised.

What this means: *Your information is also super-scrambled when we send it from our servers to your browser.*

Operational Procedures to Keep the Site Secure

We regularly audit our environments and code for security issues and apply patches expeditiously.

Everplans follows best practices to keep your data secure. We regularly audit our environments and code for security issues and apply patches expeditiously. We use commercial services that regularly check our site (including McAfee Secure) and we retain our own security experts to probe and verify the security of our site.

What this means: *We monitor everything that happens in our system and track all developer/administrative access. We also use third party services to try to poke holes in our system so we can continuously refine our security.*

Administrative Access to your Information

Our strict internal procedures prevent any Everplan employee or administrator from gaining access to your account, beyond a limited set of data necessary to help grant you access to your account (e.g. triggering confirmation emails) and restricting access to your account in urgent circumstances (e.g. limiting or removing a deputy's access). Everplans administrators can never see the plan information that you fill out or any documents that you upload. Everplans logs and regularly audits all accesses to your account, whether by you, an administrator or your deputies.

What this means: *Everplans employees do not have access to the information in your plan and only have limited access to other meta-information about your account when it's needed to help you with your account.*

Two Factor Authentication

Security is not just about protecting your data, it is also about protecting access to your account. By enabling Two Factor Authentication, whenever you sign into your Everplan from a new computer, device, or browser, we will send a unique code to your phone that you must input as part of your login.

What this means: *This extra layer of security makes sure that even if a bad guy steals your password from you (or from a site that's less secure than Everplans), he won't be able to access your Everplans.you with your account.*

SOC 2

Everplans has undergone a Type II Service Organization Control 2 (SOC 2) examination, resulting in an independent CPA's report and certification.

What this means: *A SOC 2 Type II report assures you that Everplans has established and continues to follow strict information security policies and procedures, and provides independent, third-party verification that Everplans' operations meet or exceed defined levels of processes and controls for the security of customer data.*