

Security You Can Trust

Estate⁺⁺ was designed according to the same computer system standards in use by banks and financial institutions.

Estate⁺⁺ servers are not transactional so no money can be transferred from credit cards or bank accounts. All system access is logged automatically and monitored by our system administrators.

Estate⁺⁺ leverages Amazon.com's global computing infrastructure for complete, secure, and reliable storage of your most important information.

For Your Eyes Only

Only you have access to the information stored in Estate⁺⁺. Our customer service representatives cannot view, move, upload, download, add, update, or delete any of your information.

The registration process requires you to answer a series of personal questions. These challenge questions and answers are used to verify your identity during login.

Phishing is a form of e-mail fraud that attempts to trick you into disclosing personal or financial information. Estate⁺⁺ stops phishing attempts by requesting that you verify certain personal information at login. If any information appears unfamiliar, you can terminate the login process at any time.

Sensitive personal information is hidden by encryption

Estate⁺⁺ employs a double encryption standard where data is encrypted in transmission ("*in-flight*") and in storage ("*at-rest*"). Even though Estate⁺⁺ is not a medical data application, it was designed to meet HIPAA's privacy and security standards for protected health information (PHI).

In-flight information is routed through an encrypted connection between your browser and the Estate⁺⁺ servers, known as SSL (Secure Sockets Layer). These servers cannot be accessed through an unsecured connection. This secured connection uses 128-bit encryption which has never been successfully deciphered.

At-rest information is encrypted before being stored. Estate⁺⁺ protects your information with a proprietary encryption algorithm based on the 256-bit AES/Rijndael standard.

Unattended computers get extra protection

Estate⁺⁺ protects your data even after you leave your computer. Your browser is forced to logout after 15 minutes of inactivity.

Web page caching is a browser feature that saves previously viewed information as files on the hard disk of your computer. Estate⁺⁺ prevents unwanted inspection of your valuable information by turning off web page caching on all web pages. Once you logout or close your browser these files are permanently deleted from your computer.

Autocomplete is a browser feature that saves text entries and later presents them as a list to choose from. This feature is very useful for typing in long text entries but also stores sensitive personal and financial information. Estate⁺⁺ prevents others from viewing your previously entered text entries by disabling Autocomplete on all web pages.

Be confident that information is always accurate

All data within Estate⁺⁺ is marked at the point of last update. This time and date value is generated by the server and cannot be changed. The time and date of last update appears every time data is displayed on screen or in print. All uploaded files are digitally signed to ensure file integrity.

Data integrity is guaranteed in case of an emergency. As soon as we are notified of death or incapacity your account is locked. Data can no longer be changed in any way. This action prevents unwanted changes to data by others you have allowed to use your login id or by users that have full-access to your estate.

Estate⁺⁺ leverages Amazon.com's global computing infrastructure for complete, secure, and reliable storage of your information. Data files stored within this infrastructure are both *redundant* and *distributed*. This means that multiple copies of data files (*redundant*) are stored in geographically separate locations (*distributed*). If a file is lost or destroyed in one location it is immediately available from another location.

Estate⁺⁺ further ensures the integrity of your data by creating a digital signature of each uploaded file. When a file download is requested, a second digital is created. The digital signatures must match or the file will not be downloaded.

Uploaded files are immutable. The contents of the file, the digital signature, and the upload signature (name of uploader and time of upload) cannot be changed. Uploaded files can be deleted and moved between folders. Several cosmetic attributes can be changed such as the description, medical directive indication, and validity acknowledgement. The only way to change the physical contents of an uploaded file is to delete it and upload a new copy. This ensures that uploaded files cannot be forged within the Estate⁺⁺ system.