



## Electronic Data Gathering Security Features

### Data Security

Sequoia's electronic data gathering tool is powered by a third-party software, PreciseFP. PreciseFP encrypts data on different levels so as to ensure protection. The encryption of data starts with a secure connection to and from their servers. Data is further encrypted and stored in a secured database. In the unlikely event that an intruder were to gain access to PreciseFP's servers, PreciseFP utilizes various safeguards to thereafter limit the readability of the data.

Your data is encrypted and can only be accessed by Sequoia, you, and others to whom you grant access. At any time, you are free to take your data and request a full deletion from PreciseFP's servers.

### Physical Security

PreciseFP's servers are housed in nondescript facilities located in the United States of America. These critical facilities have extensive setback and military grade perimeter control berms, as well as other natural boundary protection. Physical access is strictly controlled, both at the perimeter and at building ingress points, by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.