



Security Protocols and Procedures

For government reporting requirements and to uniquely identify each employee, ETC receives and stores social security numbers provided by employers. These numbers are used exclusively for communication between ETC, employers and the government. Internally, employees are identified by unique random identification numbers. To further ensure protection of Employee Social Security Numbers as well as any other Client Confidential Data, ETC has the following systems/procedures in place:

TX-RAMP Certification - ETC has been granted TX-RAMP Provisional Status and is working towards Level 2 compliance. We use audits and continuous monitoring to prevent and monitor intrusions and attacks. We also rigorously train all employees to ensure that security measures are implemented at every level within the company.

- **Encryption** upon receipt of data containing social security numbers.
 - ETC site utilizes HTTPS (Hyper-Text Protocol with SSL (Secure Socket Layer)). In a nutshell, this means data passed between browsers and our server is encrypted.
 - ETC SSL is certified by GeoTrust and/or GlobalSign.
 - Stored data is protected by PGP encryption.
 - Gnu Privacy Guard is a public key encryption program, it was designed to interoperate with PGP, the email encryption program. The public key can be freely distributed, and the private key is kept secret. When a file is encrypted with the public key it can only be decrypted using the private key.
 - The original creation of Gpg4win was supported by Germany's Federal Office for Information Security
- **Access** to the ETC site is restricted to authorized users.
 - To access any company or employee data, a user must login to the site.
 - Company representatives are restricted to data for their own company.
 - Failed login attempts are tracked.
 - A user id or password error incurs a time delay to prevent brute force login attempts.
 - Inactive Users are logged out with a 5-minute threshold of inactivity.
- **Tracking**
 - An Activity Log records all activities. Each log reports to the client affected and the user responsible.
 - Logins are logged.
 - Failed logins are tracked.
- **Backups**
 - Full backups are performed daily.
 - Incremental backups are performed 2 times during a normal working day, 11am & 4:00pm
 - Stored data is protected by PGP encryption.
 - Backups are housed on an off-site storage facility.
- **Audits**
 - Weekly error reports are run, and corrective measures taken, if necessary.
 - Security systems are reviewed regularly both by in-house personnel as well as independent third-party experts.
- **HIPAA/HITECH**

ETC is in compliance with HIPAA/HITECH as a Business Associate and all ETC team members with access to PHI have been trained in accordance with HIPAA/HITECH regulations and obligations and will provide a Business Associate Agreement to our Clients.
- **Social Security Numbers**
 - ETC receives social security numbers provided by employers. These numbers are used exclusively for communication between ETC, employers and the government.
 - Upon receipt, social security numbers are encrypted.
 - Only encrypted social security numbers are stored in the database.
 - Internally, employees are identified by unique random identification numbers.
 - Reports are available only to the employer and trained ETC personnel. Except when prohibited or mandated by government requirements, reports may contain redacted social security numbers.