Social Solutions
transforming human services

ETO Data Privacy

Data Privacy and Security

Social Solutions' highest priority is the protection of our client information. Use of ETO software is as secure as an on-line bank transaction. We house over 6 terabytes of client data. ETO software meets current HUD DV, HMIS, FERPA, Social Security Administration and HIPAA data management and security protocol. We maintain dozens of HIPAA Business Agreements with clients and take every precaution to ensure that data is kept confidential. We are the database of record for two national Social Security Administration initiatives. This client relationship has required that we submit to regular, unannounced comprehensive and rigorous on-site and administrative security reviews with State and Federal Government agencies – which we have passed in each instance. Our standard policy is to maintain the highest level of data privacy, security and confidentiality dictated by our clients' needs.

User Names, Passwords, and Roles

The ETO web-application utilizes user name and password functionality to prevent unauthorized application access and provide an automated audit trail of that user's interaction with the software. Users of ETO are assigned their email address as a unique user ID and strong password combinations can be enforced through the ability to set a minimum number of numeric and non alphanumeric characters that must be included in each password. The ETO web-based application is configured to detect user inactivity and will terminate a session after a defined period of time (default is 60 minutes but an administrator can change this setting) if the user does not respond to an alert prompt. In addition, each unique logon is assigned one of nine levels of access which can be customized to allow users access to particular programs and features. Role levels typically range from the System Administrator, who manages all the structural elements of the data (often as many as 100 features), to Program Managers who have access to individual and aggregate staff and client information (typically 20-30 features), to end-users who have the narrowest needs (typically 10-15 features). These levels of user access also apply to the reporting areas of the software and users only have the ability to report on the areas that they have been granted access to by their administrator. There is a complete audit trail attached to each unique user's account.

Encryption

The application is accessed by users via a secure HTTPS connection to the ETO software web application server. The HTTPS protocol which is designed to prevent eavesdropping and tampering, provides a secure communication channel to ETO application. In addition, ETO software's SQL data storage is secured by Microsoft Windows file-level encryption (EFS).

Database Security

Data housed in ETO is stored and processed separately according to sites and programs. For example, users within one partner site are not authorized to view client data collected by another partner site (unless permissions are set). Users assigned to a program can only see data for the participants, services, or outcomes associated with that program. More specifically, ETO users on the ABC program cannot access or view data belonging to an ETO user for the XYZ program without explicit permissions. This protection extends down to the program level and to specific case-load access within a program where necessary. Confidential data stored in ETO and used for projects is protected by file or volume encryption. When data is transmitted from various ETO components or locations to another, the data is also encrypted.

Fully Secure Hosted Solution

Social Solutions provides a remotely hosted Software as a Service (SaaS) solution. There are many benefits (practical & cost based) that a client will realize by using a SaaS solutions versus an in house solution. These include:

- No cost to physically maintain system (rack space, floor space, electricity, maintenance, man hours)
- No cost to enhance system (hardware upgrades, etc)
- No cost to manage the system (security, data back-up, operating system upgrades, server administration and support)
- Most Training is at no cost and available live and on-demand (except for certification program and advance reporting)
- All end-user support is included
- All upgrades are included and rolled out in a predictable schedule
- System administration time and costs will be offset by the time saved to manage your programs, efficiency gained, and more importantly the benefits your clients.
- Benefits of having your provider as a leader in performance management and access to best practices at no cost.

SunGard Data Centers

Social Solutions partners with SunGard to host the solution. The SunGard facility in Philadelphia, PA houses all the critical business systems along with the primary backup vault (EVault Recovery Appliance). The SunGard facility in Scottsdale, AZ houses the Base Vault and is used for disaster recovery. As part of this partnership Social Solution's clients receive the benefit of a world class managed and fully redundant data center infrastructure with full featured physical security measures that includes:

- Integrated closed circuit TV and card reader/biometric security system
- Man Trap security access for raised floor areas
- Exterior security cameras
- 24x7 Security Service

The ETO servers maintained at the SunGard are housed in 3 secured cages designated only for Social Solutions equipment. Only authorized users who are granted access by Social Solutions can have access to these servers.

As part of our SunGard Malicious Traffic Managed Services all of our servers have Norton Anti-Virus software installed with the following features set forth:

- Anti-virus: inbound / outbound network monitoring against known virus and worm signatures, as well as deletion of detected and/or blocked virus and worms
- Network monitoring of HTTP, HTTPS, SMTP and FTP traffic for known signatures corresponding to abnormal behavior and attacks against end users
- Spam filtering: inbound / outbound network monitoring and detection of unsolicited or spoofed SMTP and POP mail.

Best Practices/Certification

The SunGard operational process will manage the hosting, network infrastructure, storage and security of the systems. The operational structure in place are based on best practice and backed by an ITIL v3 service model that ensures all changes are repeatable and changes are managed in a controlled process. The data center infrastructure and Management processes of the hosting provider have received SAS 70 Type II as well as ISO 9001 certification and are PCI DSS-compliant facilities and processes.

Redundant Infrastructure and Backups

- 24x7x365 monitoring of uptime across the infrastructure
- Fully redundant meshed multi vendor internet Transit connectivity with diverse path for long haul access as well as fiber entry and intra-building paths. Within the building there is redundant internal network distribution.
- Redundant Utility Feeds and power backed up by dual UPS and dual power generators
- Fully redundant SAN access storage
- Social Solutions uses eVaulting technology to backup our data online with encryption which is then securely transmitted to SunGard's Scottsdale, AZ data center.

Server/Application Recovery

In case of a disaster at the SunGard facility in Philadelphia, SunGard will have ETO up and running between 24-48 hours at their Scottsdale, AZ data center.

Disaster Recovery Testing

The disaster recovery process is tested on a quarterly basis. We have never had a failure in our DR process.

Data Ownership and Access

All data is the sole and exclusive property of the client agency. Upon request and for a nominal fee, Social Solutions will provide any client with a password protected digital copy of all content collected in ETO on a password-protected CD in MS Access format.