TEXASCASA
Court Appointed Special Advocates
FOR CHILDREN

STRENGTHENING THE VOICES OF CASA STATEWIDE

Guide to Secure Transmission of Confidential Information

HHSC has required CASA programs to employ encryption to keep confidential information secure during electronic transmission. This guide offers multiple options for encryption.

Transmission of confidential information creates opportunities for unauthorized access to documents, that is, for people without the legal authority to documents to receive or review them. Document encryption protects against unauthorized access. In document encryption, a document is protected with cryptographic keys (a password) so that only individuals with the corresponding decryption keys (the same password) can open them.

Texas CASA recommends the following methods to ensure that documents, reports, files, and records remain confidential during sharing or transmission.

COURT REPORTS

Court reports are frequently shared between the volunteer advocate and the staff person who provides coaching and supervision on the case.

- Optima: Court reports can be uploaded by the Volunteer Supervisor or Volunteer into Optima for reviewing, amending or approving purposes. Optima is a secure database that is user-specific password protected. Therefore, it meets the definition of secure transmission.
- E-filing: Civil and criminal e-filing is mandated in Texas which provides the means to securely transmit CASA court reports to the court of jurisdiction.

QA REVIEWS

Texas CASA has occasion to access a program's confidential information during a QA review. To maintain confidentiality when transmitting confidential information to Texas CASA, programs should utilize the Online Data Manager (ODM) System. The ODM System is a secure, password protected site which programs access with a unique login and password. Therefore, it meets the definition of secure transmission.

The QA Review process will utilize the ODM System for the program's submission of Indicators of Compliance (IoC) documents. Texas CASA will no longer request programs to submit the IoCs via email or zip file.

Here's how to submit IoC's:

1. Login into the ODM system >
2. Go to the QA Reviews tab >
3. Double click on the current fiscal year QA review >
4. Click on Notes and Attachments >
5. Click on Upload files >
6. Select files to upload.

Uploading files to the ODM is quick and easy. Texas CASA will delete any confidential records or documents upon the conclusion of the QA review.

ENCRYPTION VIA PASSWORD PROTECTING DOCUMENTS

Current versions of Microsoft Office, Adobe Acrobat and WinZip offer password protection to secure your files. When emailing a Word or Excel document with confidential or identifying information, use the password protection feature.

Here's how to password protect a document:

1. Open the Word, Excel or PDF document>
2. Click File>
3. Click Protect Document>
4. Click Encrypt with Password>
5. Enter your password.

It is recommended that your program use a strong password so if the document is received by an unintended person, it will remain locked and be impossible to open or view without the password.

Choosing Passwords

Choose something your volunteer will know and be able to remember—a unique identifier significant to them, that others would not know. This password can be recorded in Optima within the volunteer file. Optima is secure place to keep a record of each volunteer's unique password. Remember that weak passwords are easy to crack.

Adobe Acrobat Security Envelopes

Adobe Acrobat includes "security envelopes" that can be used to protect multiple files placed as attachments in an encrypted "envelope." Information is secure if confidential information is placed within such password-protected attachments, instead of in the body of the email.

Here's how to password protect a PDF:

1. Open the PDF in Acrobat>
2. Go to File, then click "Protect Using Password">
3. Set the password for editing the PDF or only for viewing it>
4. Type your password, then re-type it>
5. Click "Apply."

ENCRYPTION VIA A PAID SERVICE

CASA programs can subscribe to an encryption service to provide confidentiality for emails. Encryption transforms readable data into unreadable data and requires a key to make data readable again. It all happens automatically via encryption software. Encryption can be used to protect data at rest, such as data stored on servers or devices, and data in motion, such as information transmitted through networks, the internet and cellphones.

If you're using an office productivity suite such as Google G Suite or Microsoft Office 365, both offer optional email encryption.

Another option is Transport Layer Security (TLS), which creates a secure environment for web browsing, emailing or other client-server applications. TLS is commonly used to secure web servers, allowing safe online transactions that are identified by a padlock icon in a browser's address bar. When applied to email servers, TLS provides encryption from one email gateway to another. Setup requires a digital certificate through a third-party certificate authority that confirms the authenticity of the servers. While an industry standard for safety, TLS protection can be lost if emails are copied to or forwarded to recipients using systems that do not support TLS.

CONFIDENTIALITY WHILE TEXTING

When texting about a case, remember to use non-specific, non-identifying information. For example, when communicating about Jim Johnson, you can use just the first name (Jim) or first initial with last name (J. Johnson) with no other identifying information. If the text or email is sent to an unintended recipient, they will not have received identifying information, minimizing the risk of a confidentiality breach.

Another way to ensure data integrity during transmission is to establish network communication protocols. All devices should be password protected. Biometric identifiers, such as a fingerprint, facial recognition, or voice pattern, offer the greatest protect for digital devices such as tablets, cell phones, and computers.

CONFIDENTIALITY NOTICE FOR EMAIL TRANSMISSIONS

Email transmissions from CASA programs should also have a confidentiality notice located at the bottom of each email below the signature line. All staff should include a confidentiality notice in the footer of their email. Instructions for editing a footer in Outlook can be found at: https://support.microsoft.com/en-gb/office/change-an-email-signature-86597769-e4df-4320-b219-39d6e1a9e87b

See the sample below:

"CONFIDENTIALITY NOTICE: This email communication and any attachments may contain confidential and privileged information for the use of the designated recipients named above. This transmission is strictly confidential. If you are not the intended recipient of this message, you may not disclose, print, copy or disseminate this information. If you have received this in error, please reply and notify the sender (only) and delete the message. Unauthorized interception of this email is a violation of the Electronic Communications Privacy Act, 18 U.S.C. §2510-2521."

INFORMATION DESTRUCTION POLICY

An information destruction policy is a formal, written policy that directs board, staff and volunteers to securely dispose of documents, files, texts, emails, and photographs containing case information after case closure. Confidential information not stored in the program's secure database should be kept in a locked or secure location, during and after case closure.